

User Guide

WR850 Wireless Broadband Routers WR850GP and WR850G



MOTOROLA
intelligence everywhere™



WR850G



WR850GP

WARNING: TO PREVENT FIRE OR SHOCK HAZARD, DO NOT EXPOSE THIS PRODUCT TO RAIN OR MOISTURE. THE UNIT MUST NOT BE EXPOSED TO DRIPPING OR SPLASHING. DO NOT PLACE OBJECTS FILLED WITH LIQUIDS, SUCH AS VASES, ON THE UNIT.

CAUTION: TO ENSURE REGULATORY COMPLIANCE, USE ONLY THE PROVIDED POWER AND INTERFACE CABLES.

CAUTION: DO NOT OPEN THE UNIT. DO NOT PERFORM ANY SERVICING OTHER THAN THAT CONTAINED IN THE INSTALLATION AND TROUBLESHOOTING INSTRUCTIONS. REFER ALL SERVICING TO QUALIFIED SERVICE PERSONNEL.

This device must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product.

Postpone router installation until there is no risk of thunderstorm or lightning activity in the area.

Do not overload outlets or extension cords, as this can result in a risk of fire or electric shock. Overloaded AC outlets, extension cords, frayed power cords, damaged or cracked wire insulation, and broken plugs are dangerous. They may result in a shock or fire hazard.

Route power supply cords so that they are not likely to be walked on or pinched by items placed upon or against them. Pay particular attention to cords where they are attached to plugs and convenience receptacles, and examine the point where they exit from the product.

Place this equipment in a location that is close enough to an electrical outlet to accommodate the length of the power cord.

Place this equipment on a stable surface.

When using this device, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- Read all of the instructions {listed here and/or in the user manual} before you operate this equipment. Give particular attention to all safety precautions. Retain the instructions for future reference.
- Comply with all warning and caution statements in the instructions. Observe all warning and caution symbols that are affixed to this equipment.
- Comply with all instructions that accompany this equipment.
- Avoid using this product during an electrical storm. There may be a risk of electric shock from lightning. For added protection for this product during a lightning storm, or when it is left unattended and unused for long periods of time, unplug it from the wall outlet, and disconnect the cable system. This will prevent damage to the product due to lightning and power surges.
- Operate this product only from the type of power source indicated on the product's marking label. If you are not sure of the type of power supplied to your home, consult your dealer or local power company.
- Upon completion of any service or repairs to this product, ask the service technician to perform safety checks to determine that the product is in safe operating condition.

It is recommended that the customer install an AC surge protector in the AC outlet to which this device is connected. This is to avoid damaging the equipment by local lightning strikes and other electrical surges.

Different types of cord sets may be used for connections to the main supply circuit. Use only a main line cord that complies with all applicable product safety requirements of the country of use.

Installation of this product must be in accordance with national wiring codes.

Place unit to allow for easy access when disconnecting the power cord/adaptor of the device from the AC wall outlet.

Wipe the unit with a clean, dry cloth. Never use cleaning fluid or similar chemicals. Do not spray cleaners directly on the unit or use forced air to remove dust.

This product was qualified under test conditions that included the use of the supplied cables between system components. To be in compliance with regulations, the user must use these cables and install them properly. Connect the unit to a grounding type AC wall outlet using the power adapter supplied with the unit.

Do not cover the device, or block the airflow to the device with any other objects. Keep the device away from excessive heat and humidity and keep the device free from vibration and dust.

Installation must at all times conform to local regulations.

FCC Compliance Class B Digital Device

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CAUTION: Changes or modifications not expressly approved by Motorola for compliance could void the user's authority to operate the equipment.

Canadian Compliance

This Class B digital apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations. Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

FCC Declaration of Conformity

Motorola, Inc., Broadband Communications Sector, 101 Tournament Drive, Horsham, PA 19044, 1-215-323-1000, declares under sole responsibility that the WR850G/GP, WE800G, WA840G/GP, WN825G/GP, WPCI810G/GP, WU830G, and BR700 comply with 47 CFR Parts 2 and 15 of the FCC Rules as Class B digital devices. These devices comply with Part 15 of FCC Rules. Operation of these devices is subject to the following two conditions: (1) These devices may not cause harmful interference, and (2) these devices must accept any interference that may cause undesired operation.

Wireless LAN Information

The WR850G/GP, WE800G, WA840G/GP, WN825G/GP, WPCI810G/GP, and WU830G Wireless LAN products are wireless network products that use Direct Sequence Spread Spectrum (DSSS) radio technology. These products are designed to be inter-operable with any other wireless DSSS type product that complies with:

- The IEEE 802.11 Standard on Wireless LANs (Revision B and Revision G), as defined and approved by the Institute of Electrical Electronics Engineers.
- The Wireless Fidelity (WiFi) certification as defined by the Wireless Ethernet Compatibility Alliance (WECA).

Wireless LAN and your Health

The WR850G/GP, WE800G, WA840G/GP, WN825G/GP, WPCI810G/GP, and WU830G, like other radio devices, emit radio frequency electromagnetic energy, but operate within the guidelines found in radio frequency safety standards and recommendations.

Restrictions on Use of Wireless Devices

In some situations or environments, the use of wireless devices may be restricted by the proprietor of the building or responsible representatives of the organization. For example, using wireless equipment in any environment where the risk of interference to other devices or services is perceived or identified as harmful.

If you are uncertain of the applicable policy for the use of wireless equipment in a specific organization or environment, you are encouraged to ask for authorization to use the device prior to turning on the equipment.

The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of the devices included with this product, or the substitution or attachment of connecting cables and equipment other than specified by the manufacturer. Correction of interference caused by such unauthorized modification, substitution, or attachment is the responsibility of the user.

The manufacturer and its authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from failing to comply with these guidelines.

FCC Certification

The WR850G/GP, WE800G, WA840G/GP, WN825G/GP, WPCI810G/GP, and WU830G contain a radio transmitter and accordingly have been certified as compliant with 47 CFR Part 15 of the FCC Rules for intentional radiators. Products that contain a radio transmitter are labeled with FCC ID and the FCC logo.

Caution: Exposure to Radio Frequency Radiation.

To comply with the FCC RF exposure compliance requirements, the separation distance between the antenna and any person's body (including hands, wrists, feet and ankles) must be at least 20 cm (8 inches).

Canada - Industry Canada (IC)

The wireless radio of this device complies with RSS 210 and RSS 102 of Industry Canada.

This Class B digital device complies with Canadian ICES-003 (NMB-003).

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Copyright © 2005 Motorola, Inc.

All rights reserved. No part of this publication may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation or adaptation) without written permission from Motorola, Inc.

Motorola reserves the right to revise this publication and to make changes in content from time to time without obligation on the part of Motorola to provide notification of such revision or change. Motorola provides this guide without warranty of any kind, either implied or expressed, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Motorola may make improvements or changes in the product(s) described in this manual at any time.

MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. Microsoft, Windows, Windows Me, Windows XP, Windows 95, Windows 98, Windows NT, Windows 2000, DirectX, MSN, and NetMeeting are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Microsoft Windows screen shots are used by permission of Microsoft Corporation. Wi-Fi is a registered trademark of Wireless Ethernet Compatibility Alliance, Inc. AOL is a registered trademark and Instant Messenger is a trademark of America Online, Inc. QuickTime is a registered trademark of Apple Computer, Inc. Net2Phone is a registered trademark of Net2Phone, Inc. Battle.net is a registered trademark of Blizzard Entertainment. Unix is a registered trademark of The Open Group. The following websites are not sponsored, affiliated, or controlled by Motorola: www.dyndns.org, www.changeip.com, and www.ntp.org. All other product or service names are the property of their respective owners.

Contents

Section 1: Overview 1-1

Understanding Your User Guide.....	1-3
Box Contents.....	1-3
Understanding Functions.....	1-4
Router	1-4
LAN.....	1-4
TCP/IP	1-4
<i>Static IP Address</i>	<i>1-4</i>
<i>Dynamic IP Address</i>	<i>1-5</i>
DHCP Server	1-5
Sample Home Network Diagram	1-5
Router Physical Description	1-6
Back of Router	1-6
Front of Router.....	1-7
LED Description	1-8

Section 2: Installation 2-1

Physical Installation of the WR850	2-1
Positioning Your Router for Optimal Wireless Performance.....	2-1
Hardware Setup	2-2
<i>Antenna Installation</i>	<i>2-2</i>
<i>Physical Placement.....</i>	<i>2-2</i>
<i>Electrical Connection</i>	<i>2-6</i>
Establishing Your First Connection to the WR850.....	2-7
Easy Install Process.....	2-7
Manual Install – Wired Connection	2-7
Manual Install – Wireless Connection	2-8
Configuring Computers to Communicate with the WR850	2-11
<i>Configuring Windows 98SE and ME.....</i>	<i>2-12</i>
<i>Configuring Windows 2000.....</i>	<i>2-14</i>
<i>Configuring Windows XP.....</i>	<i>2-17</i>

Section 3: Configuration 3-1

Accessing the Web-Based Configuration Utility	3-2
Logging In	3-2
Overview of Configuration Pages.....	3-3
Navigation Between Pages.....	3-3
The BASIC Configuration Page.....	3-4
BASIC Page – Commonly Used Configuration Options.....	3-4

BASIC Page – All Configuration Options	3-6
<i>Options related to: CONTROLLING ACCESS TO THE CONFIGURATION UTILITY</i>	<i>3-6</i>
<i>Options related to: ENABLING PRIMARY ROUTER FUNCTIONS</i>	<i>3-6</i>
<i>Options related to: ENABLING TIME-RELATED FUNCTIONS</i>	<i>3-8</i>
<i>Options related to: LOGGING WR850 ACTIVITY</i>	<i>3-9</i>
BASIC Page Action Buttons.....	3-10
The LAN (Local Area Network) Configuration Page	3-11
LAN Page – Commonly Used Configuration Options	3-11
LAN Page – All Configuration Options	3-12
<i>Options related to: SELECTING THE WR850 LOCAL AREA NETWORK</i>	
<i>PROTOCOL</i>	<i>3-12</i>
<i>Options related to: ENABLING THE WR850 BUILT-IN DHCP SERVER</i>	<i>3-13</i>
<i>Options related to: OPTIMIZING LOCAL AREA NETWORK ROUTING</i>	<i>3-14</i>
LAN Page Action Buttons	3-15
The WAN (Wide Area Network) Configuration Page	3-16
WAN Page – All Configuration Options	3-18
<i>Options related to: SELECTING THE WR850 BROADBAND CONNECTION</i>	
<i>MODE.....</i>	<i>3-18</i>
<i>Options related to: SETTING UP A STATIC BROADBAND CONNECTION</i>	<i>3-19</i>
<i>Options related to: SETTING UP A PPPoE BROADBAND CONNECTION</i>	<i>3-20</i>
<i>Options related to: SETTING UP A LINK TO A DYNAMIC DOMAIN NAME</i>	
<i>SERVICE.....</i>	<i>3-22</i>
<i>Options related to: OPTIMIZING WAN ROUTING.....</i>	<i>3-23</i>
WAN Page Action Buttons	3-24
The STATUS Configuration Page	3-25
STATUS Page Configuration Options.....	3-25
The FILTERS Configuration Page.....	3-26
FILTERS Page – Commonly Used Configuration Options.....	3-26
FILTERS Page – All Configuration Options	3-27
FILTERS Page Action Buttons.....	3-29
FILTERS Page Examples – Establishing Parental Controls on Internet Use.....	3-30
<i>Blocking Internet Use at All Times – LAN DHCP Server Enabled</i>	<i>3-30</i>
<i>Blocking Internet Use at All Times – LAN DHCP Server Disabled</i>	<i>3-31</i>
<i>Blocking Internet Use at Particular Times</i>	<i>3-32</i>
<i>Blocking Specific Types of Internet Use at Particular Times.....</i>	<i>3-34</i>
The ROUTING Configuration Page	3-36
ROUTING Page – Commonly Used Configuration Options	3-37
ROUTING Page – All Configuration Options	3-37
ROUTING Page Action Buttons.....	3-41
The WIRELESS Configuration Page.....	3-42
WIRELESS Page – Commonly Used Configuration Options	3-45
WIRELESS Page – All Configuration Options	3-46
<i>Options related to: ESTABLISHING YOUR WIRELESS NETWORK</i>	<i>3-46</i>
<i>Options related to: ENSURING INTEROPERABILITY WITH WIRELESS DEVICES.....</i>	<i>3-47</i>
<i>Options related to: CUSTOMIZING WIRELESS DATA THROUGHPUT</i>	<i>3-48</i>

Contents

Options related to: OPTIMIZING WIRELESS OPERATION FOR YOUR ENVIRONMENT.....	3-49
Options related to: BOOSTING WIRELESS PERFORMANCE	3-50
Options related to: OPTIMIZING WIRELESS PERFORMANCE FOR MULTIMEDIA	3-51
Options related to: CONFIGURING THE WR850 AS A WIRELESS BRIDGE	3-53
Options related to: RESTRICTING WIRELESS ACCESS TO SPECIFIC USERS.....	3-55
WIRELESS Page Action Buttons	3-56
The SECURITY Configuration Page.....	3-57
SECURITY Page – Recommended Configuration Options.....	3-59
SECURITY Page – All Configuration Options	3-61
Options related to: SELECTING WIRELESS AUTHENTICATION METHODS	3-61
Options related to: ENABLING WIRELESS ENCRYPTION METHODS	3-64
Options related to: SETTING UP COMPATIBILITY WITH A RADIUS SERVER.....	3-66
SECURITY Page Action Buttons	3-67
SECURITY Page Example – Matching Settings in the WR850 and Wireless Clients	3-68
The FIRMWARE Configuration Page	3-72
FIRMWARE Page Configuration Options.....	3-72

Section 4: Troubleshooting 4-1

Contact Us	4-1
Hardware Solutions	4-1
My computer is experiencing difficulty in connecting to the router.....	4-2
My broadband modem already uses a built-in router.....	4-2
Software Solutions.....	4-3
I would like to test to see if my Internet connection is live.	4-3
I cannot access the Web-based Configuration Utility for the router.....	4-4
How do I extend my wireless network to cover more area?	4-4
I cannot browse past the first screen of the Web-based Configuration Utility.....	4-4
How do I match WEP keys between the router and my wireless clients?	4-5

Section 5: Glossary 5-1

Section 1: Overview

Congratulations on purchasing the Motorola® WR850GP Wireless Broadband Router or Motorola WR850G Wireless Broadband Router.¹

The WR850 includes both an 802.11b/g wireless access point and a 4-port Ethernet router. So it is both wireless and wired, providing the foundation for a truly customized network full of options.

Using the WR850, you can share files, pictures, peripherals, printers and more with everyone else on the network. By connecting a broadband modem (cable, DSL or other), you can also share a single high speed Internet connection.

The WR850 offers both the popular 802.11b wireless standard as well as the nearly 5-times-faster 802.11g standard, providing you the ultimate in flexibility and speed. With Wi-Fi® Protected Access (WPA™) included, your wireless connections are robust and secure, giving you the security to communicate without fear that your signal might be compromised.

The WR850GP comes loaded with Performance Enhancement technology that accelerates your wireless network and your fun. This new technology boosts wireless performance among compatible Motorola devices up to 35% faster than over standard 802.11g networking.

Upgradeable firmware keeps the router's control software up-to-date. The WR850 captures the latest technology in a package that stays current, protects your home network, and provides you easy home network management.

Wireless Broadband Router WR850GP

Wireless Broadband Router WR850G



¹ Unless otherwise stated, this User Guide will use WR850 as the generic term for both the WR850G and WR850GP

Your wireless router is really several products built into one router:

Wireless Access Point

- Connects your router to your laptop wirelessly and allows you to roam unfettered
- Supports a multitude of devices that operate with both 802.11g and 802.11b wireless communication standards
- Protects your wireless communications using Wi-Fi Protected Access (WPA), Wi-Fi Protected Access version 2 (WPA2™), 802.1X, and Wired Equivalent Privacy (WEP) security algorithms
- Supports peer-to-peer communication using built-in Wireless Distribution System (WDS) functionality

4-port Full Duplex 10/100 Ethernet Switch and Router

- Supports wired connection of up to 4 computers or devices
- Shares a broadband Internet (cable, DSL, or other) connection with each of your networked devices
- Enables you to form a Local Area Network (LAN)

Security and Protection

- Protects against Internet intruders with a built-in firewall
- Hides your LAN IP addresses and devices from the Internet, using Network Address Translation (NAT) and IP and/or MAC Address filtering
- Frees you to connect to your corporate network, with Virtual Private Network (VPN) compatibility

Understanding Your User Guide

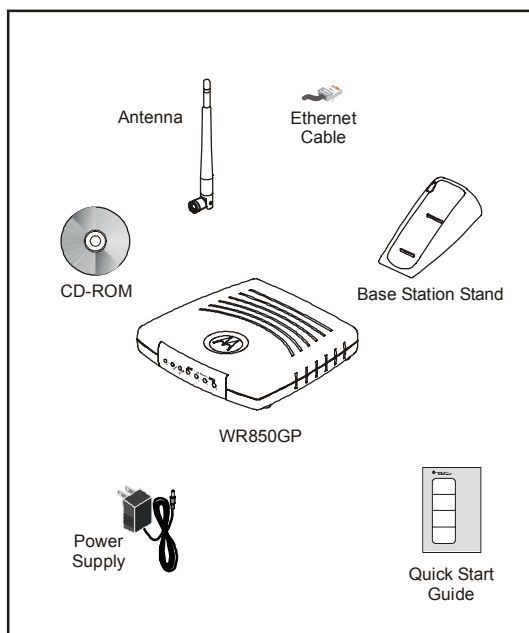
The User Guide is divided into the following sections:

Overview	Describes the router and its functions, the technology used, and the recommended methods for positioning the router.
Installation	<p>It is assumed that you will use the Installation Wizard on the CD-ROM to set up your router. If not, refer to this section for instructions on getting your router up and running.</p> <p>After you have completed this section, your router will be active and ready to work.</p>
Configuration	Describes the Web-based Configuration Utility, which can be used for advanced customization or re-configuration of the WR850.
Troubleshooting	Details helpful solutions to common router problems.
Glossary	List of terms and acronyms.

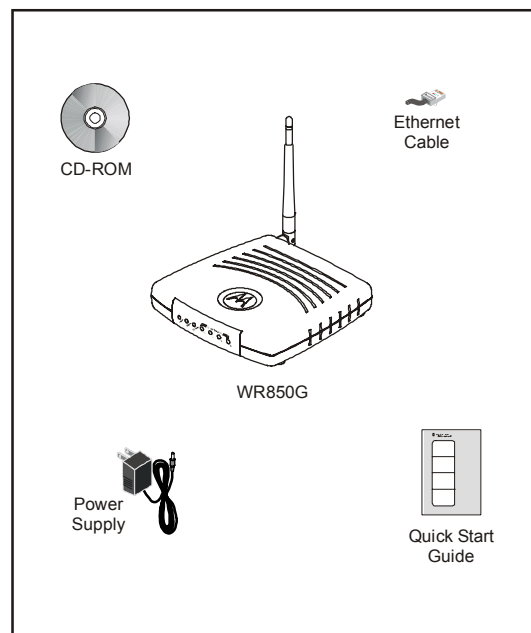
Box Contents

Your box contains the following:

WR850GP



WR850G



Understanding Functions

Before installing your wireless router, please take a few minutes to review the wireless networking functions described in this section.

Router

Generally, routers connect two networks together. The WR850 connects your home network with the Internet, which can be thought of as a very large network.

The router's firewall inspects each packet of data as it flows in from the internet before delivering it to the appropriate PC. Network Address Translation (NAT) protects the privacy of the IP addresses of devices on your home network, by translating them into a single address when visible to the public internet. This is how your network remains protected and private on the Internet.

LAN

Local Area Network. A local area network provides a full-time, high-bandwidth connection over a limited area such as a home, building, or campus. Ethernet is the most widely used LAN standard.

TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) comprises the backbone of the Internet. IP moves packets of data between nodes while TCP verifies delivery from client to server. Every device you hook up to your wireless router identifies itself with an IP address. You are able to assign devices on your network with either a static or dynamically assigned IP address.

Static IP Address

A static IP address is a fixed address that is assigned manually to a device on the network. Static IP addresses must be unique and cannot be shared, therefore they are used in situations where the address should never change, like print servers or PC servers.

If you are using your wireless router to share an Internet connection, your Internet Service Provider (ISP) might have assigned you a static IP address, which you will use when configuring your router. See Section 3: Configuration.

Dynamic IP Address

A dynamic IP address is a temporary IP number, dynamically or randomly generated by a DHCP server. The address lasts only as long as the server allots, usually in the space of a day or two. When the IP address expires, the client is automatically reassigned a new IP address, ensuring smooth communication.

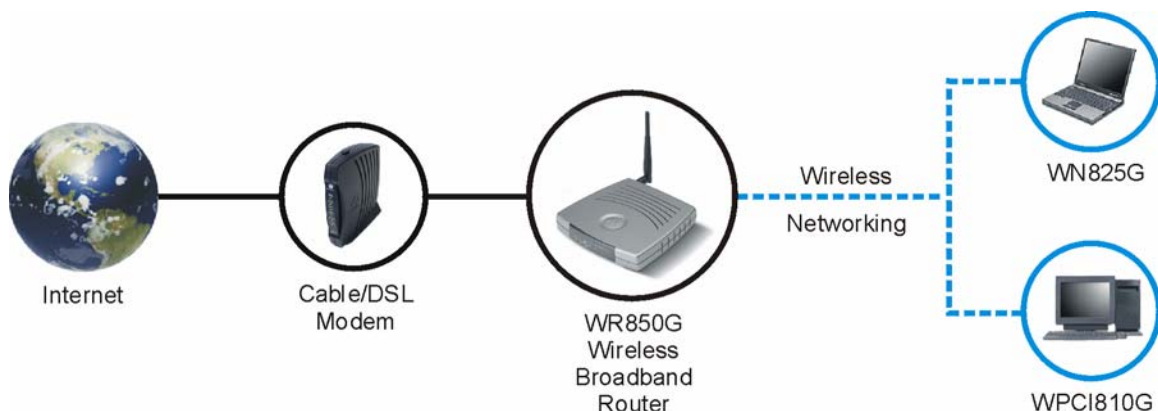
If you are using your wireless router to share an Internet connection, your ISP might have assigned you a dynamic IP address, which you use when configuring your router. See Section 3: Configuration.

DHCP Server

A Dynamic Host Configuration Protocol (DHCP) Server assigns IP addresses to clients connected to the router. A *client* is any device that can connect with your router. The client (PC, gaming device, etc.) is automatically assigned an IP address every time a device is added to your network, which frees you from manually assigning IP addresses.

Sample Home Network Diagram

Your wireless router serves as the centerpiece of your network, allowing you to share files, printers, and the Internet connection. A sample home network is shown below:



The Internet communicates with the modem, which in turn communicates with the router. The router acts as the gateway to your network; it sends devices information such as requests for Internet access, file sharing, or multiplayer games. The router controls the information for your network, intelligently routing the information to its required destination while at the same time protecting your network from the public domain.

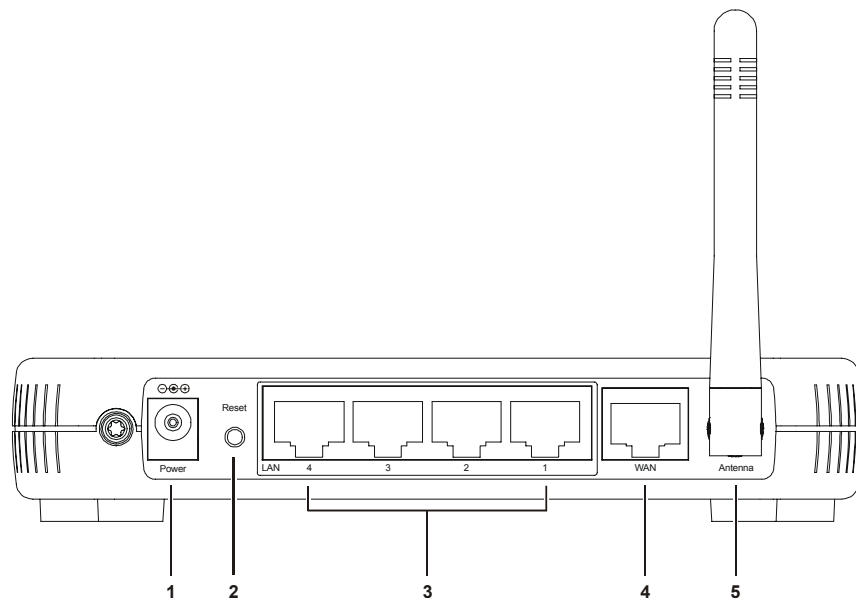
Router Physical Description

The following sections describe the physical characteristics of your router.

For instructions on installing your router, see Section 2: Installation.

Back of Router

The following illustration shows the WR850 back panel:

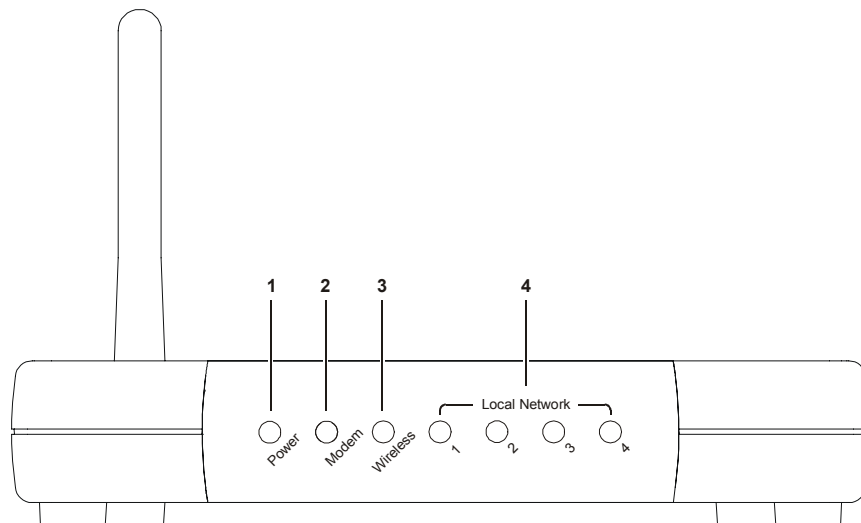


Feature	Description
1 Power	The receptacle where you plug in the power adapter.
2 Reset Button	<p>Resets your router or resets the router to the default login settings.</p> <p>If the router experiences trouble connecting to the Internet, briefly press and release the Reset button to reset the router. This retains the router's configuration information.</p> <p>To reset the router to the factory defaults, press and hold the Reset button for more than five seconds. This clears the router's Username, Password, IP Address, Subnet Mask and Operation Mode. To re-configure the router, see Section 3: Configuration.</p>

	Feature	Description
3	LAN Ports 1-4	<p>These four ports connect the router to your LAN or home network using Ethernet cables. This enables communication among clients, such as PCs or print servers, on the network. The LAN ports support either 10-BASE-T or 100-BASE-T transmission speeds as well as straight-through and crossover Ethernet cables.</p> <p>Any of these four ports can also serve as an uplink port to other network devices, such as another router or switch, which allows you to extend your network.</p>
4	WAN	<p>Connect your modem to your router using this port with your supplied Ethernet cable. This is the only port you can use for this procedure. This enables your router to access the Internet. The port supports 10/100 Mbps as well as straight-through and crossover Ethernet cables.</p>
5	Antenna	<p>The antenna is used for wireless connections. You are able to rotate the antenna to gain the best signal reception.</p>

Front of Router

The following illustration shows the WR850 front panel:

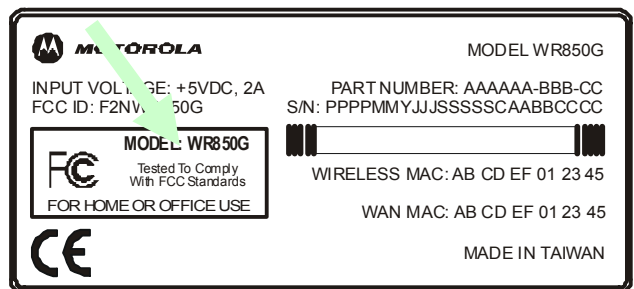


The LEDs of the router indicate its operational status.

LED Description

LED	Condition	Color	Status
1 Power	ON	Green	The device is powered on and operating normally.
	ON	Red	The Power LED turns RED as soon as the reset button is depressed. If the reset button is held down, the LED starts to blink RED and the router's username, password, private LAN IP address, private subnet mask address and operation mode are restored to factory default settings. If the Power LED stays RED for longer than 5 seconds, this indicates that the firmware is corrupted and needs to be restored.
2 Modem	OFF	None	The device is not powered on.
	ON/Blinking	Amber	10BaseT link detected / <u>active traffic present</u> .
	ON/Blinking	Green	100BaseT link detected / <u>active traffic present</u> .
	OFF	None	No external Ethernet device has been attached and detected. The Ethernet link may be down.
3 Wireless	ON/Blinking	Green	The wireless interface is enabled / <u>active traffic present</u> .

NOTE: The wireless LED does not blink on WR850G "Version 1" hardware. You can determine your version of hardware by looking at the product label on the bottom of the router. Within the box that includes the FCC logo, a "Version 1" unit will display "MODEL: WR850G", while a "Version 2" unit will display "MODEL: WR850Gv2" (see example below).



	OFF	None	The wireless interface is not enabled by the firmware.
4 LAN (x4)	ON/Blinking	Amber	10BaseT link detected / <u>active traffic present</u> .
	ON/Blinking	Green	100BaseT link detected / <u>active traffic present</u> .
	OFF	None	No external Ethernet device has been attached and detected. The Ethernet link may be down.

Section 2: Installation

This section will help you:

- physically install your WR850, and
- establish a first connection between a PC and the WR850.

Once this first connection is made, you can configure the WR850 to support all of the other wired and/or wireless connections you need.

Physical Installation of the WR850

Positioning Your Router for Optimal Wireless Performance

Your wireless router uses a radio transmission technology defined by the Institute of Electrical and Electronics Engineers (IEEE) called 802.11 Wireless Fidelity (Wi-Fi). This standard is subdivided into distinct categories of speed and the frequency spectrum used, designated by the lower case letter after the standard.

For example, your router supports both the 'b' and 'g' specifications. The 802.11b specification transmits data rates up to 11 Mbps while the 802.11g specification transmits data rates up to 54 Mbps. These are theoretical standards so your performance may vary. The radio waves radiate out in a donut-shaped pattern. The waves travel through walls and floors, but transmission power and distance are affected. The theoretical distance limit is 1,000 feet (305 meters), but actual throughput and distance varies.

Both standards operate in the 2.4 GHz range, meaning other electrical appliances also might interfere with the router – televisions, radios, microwave ovens, or 2.4 GHz cordless telephones. Therefore, positioning your router where it encounters the least interference helps maintain a better connection.

The following lists the expected wireless range of the router. This table is only a guide and coverage varies due to local conditions.

Data Rate	Open Area	Closed Area
54 Mbps	Up to 100 ft (30m)	Up to 60 ft (18m)
11 Mbps	Up to 900 feet (275 m)	Up to 160 feet (49 m)
5.5 Mbps	Up to 1300 feet (396 m)	Up to 200 feet (61 m)
2 or 1 Mbps	Up to 1500 feet (457 m)	Up to 300 feet (91 m)

To achieve the best wireless performance, review these guidelines before deciding where to place your router:

- Placing your base station in the physical center of your network is the best location because the antenna sends out the signal in all directions.

- Placing the router in a higher location, such as on top of a cabinet, helps disperse the signal cleanly, especially to receiving locations on upper stories.
- If possible, position your router so there is direct line of sight between the router and your other home network devices.
- Avoid placing the router next to large solid objects like computer cases, monitors, walls, fireplaces, etc. This helps the signal penetrate more cleanly.
- Other wireless devices like televisions, radios, microwaves, and 2.4 GHz cordless telephones can interfere with the signal. Keep these devices away from the router.
- Mirrors, especially silver-coated, can reduce transmission performance.

Hardware Setup

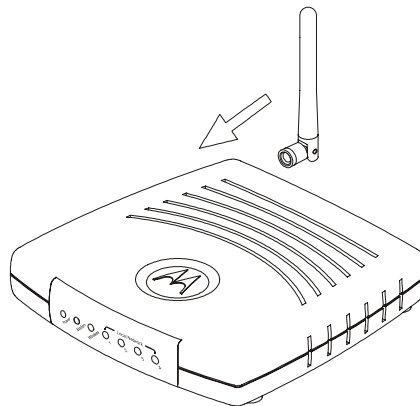
Hardware setup includes:

- Antenna Installation: connecting the antenna to the router
- Physical Placement: how and where you physically place your router
- Electrical Connection: how to connect the power cord

Antenna Installation

When shipped, the antenna for the WR850GP is not connected to the router. To attach the antenna to the router:

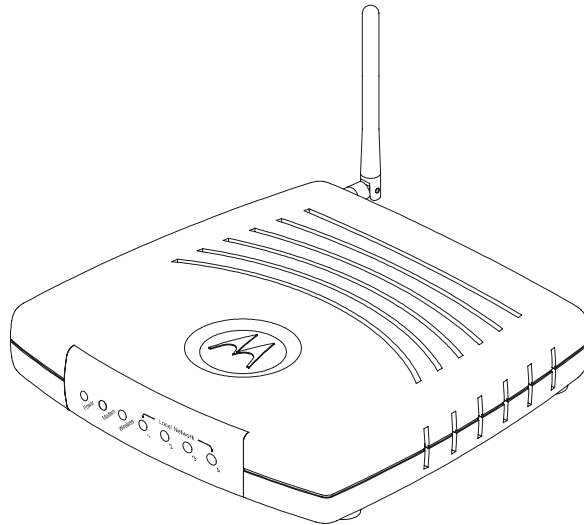
- 1 Locate the antenna port on the back of the router (the threaded knob).
- 2 Screw the antenna connector clockwise on to the threaded knob until firmly seated. Do not over-tighten.



Physical Placement

For desktop use, the WR850GP can be installed either horizontally or vertically. The WR850G can only be installed horizontally.

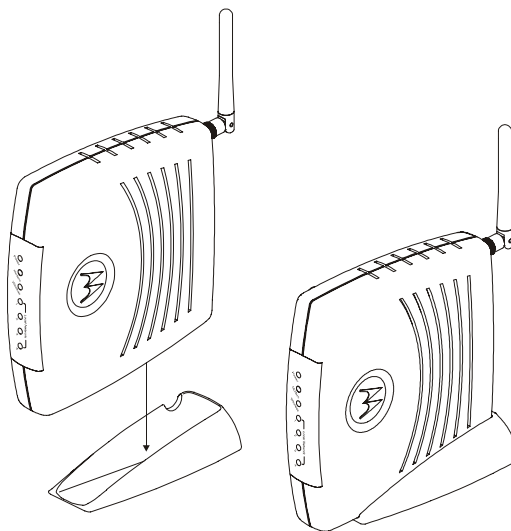
Either router can also be mounted on a wall.

Horizontal Installation

- 1 Place the router in the desired location and follow the procedures below for connecting and configuring the router.

Vertical Installation

(WR850GP only)



- 1 Insert the router into the supplied base. Ensure that the antenna's location is on top. The router's foot slides snugly into a notch in the base to keep the router stable.
- 2 Follow the installation procedures for connecting and configuring the router.

Wall Mount Installation

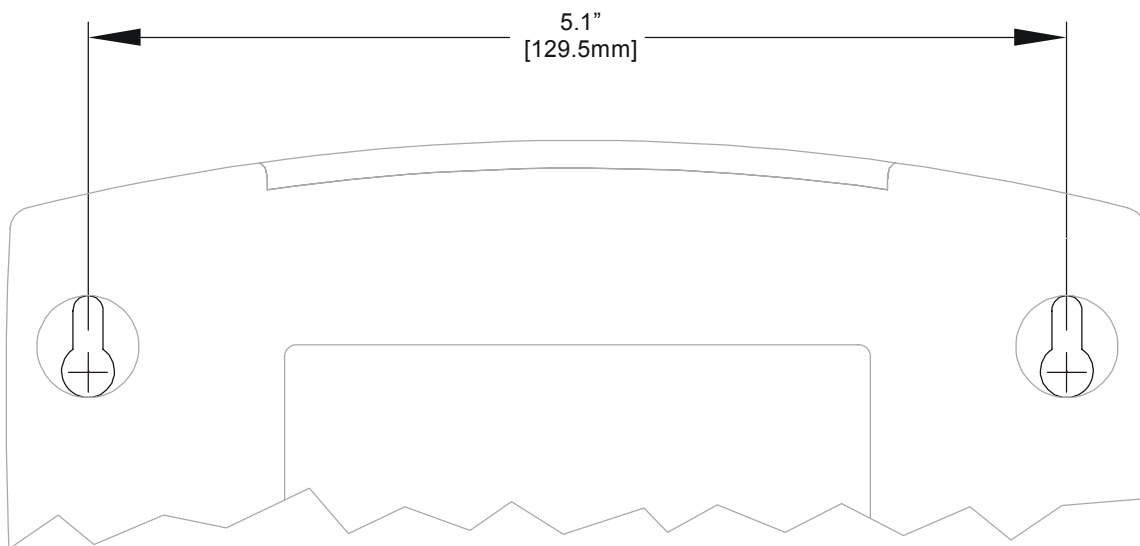
If you mount the router on the wall, you must:

- Position the router as specified by the local or national codes governing residential or business communications services.
- Follow all local standards for installing a network interface router/network interface device (NIU/NID).

If possible, mount the router to concrete, masonry, a wooden stud, or other solid wall material. Use anchors when necessary; for example if you must mount the router on drywall.

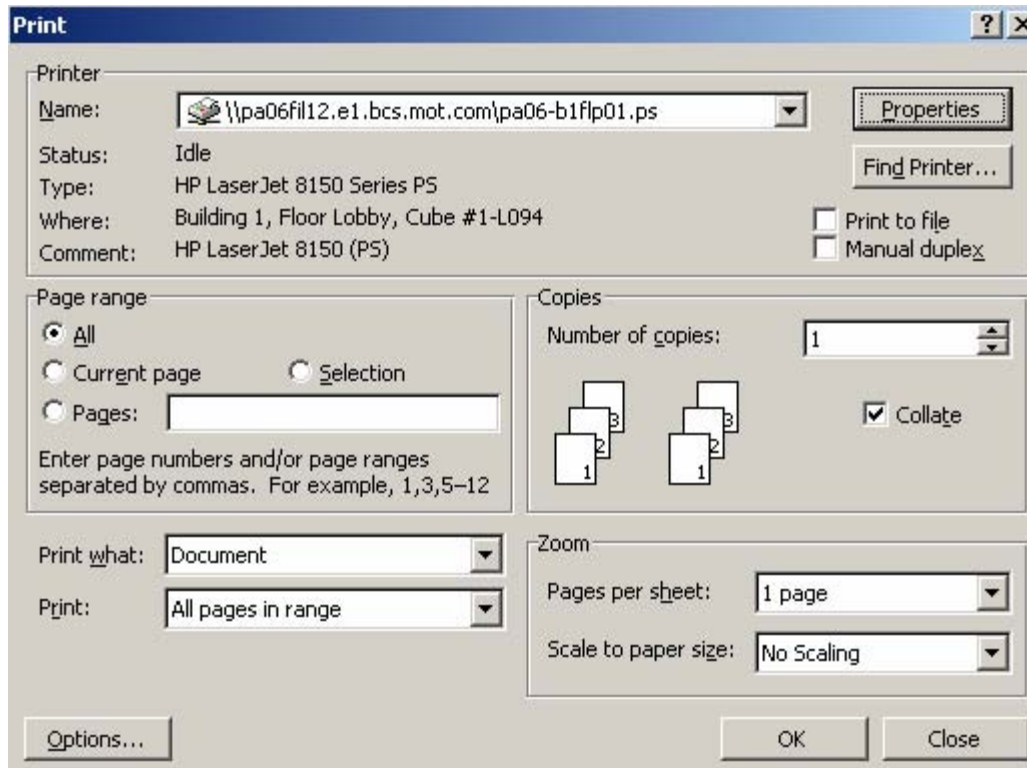
To mount your router on the wall:

- 1 Print the Wall Mounting Template shown on this page:



The illustration is drawn at a one-to-one scale, which means that when printed, it provides the exact dimensions required to mount the router.

- 2 To print the Wall Mounting Template, click the **Print** icon or choose **Print** from the File menu.



- 3 In both the *Pages from* and *to* fields, enter the page number on which the Wall Mounting Template appears.
- 4 Click **OK**.
- 5 Measure the printed template with a ruler to ensure that it is the same size as the template on page 2-3.
- 6 Use a center punch to mark the center of the holes on the wall.
- 7 On the wall, locate the marks for the mounting holes you just made.

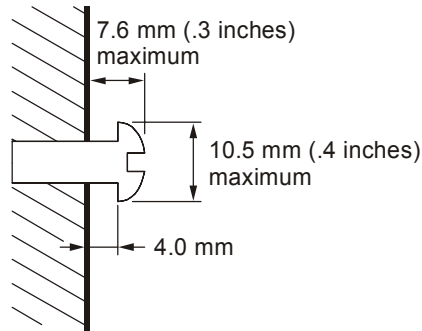
WARNING!



Before drilling holes, check the structure for potential damage to water, gas, or electric lines.

- 8 Drill the holes to a depth of at least 3.8 cm (1½ inches).
- 9 If necessary, seat an anchor in each hole. Use M5 x 38 mm (#10-16 x 1½ inch) screws with a flat underside and maximum screw head diameter of 10.5 mm to mount the router.

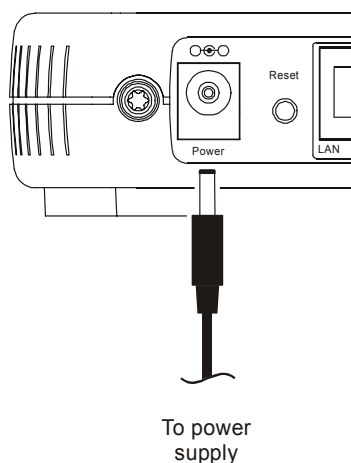
- 10** Using a screwdriver, turn each screw until part of it protrudes from the wall, as shown:
- There must be 4.0 mm (.16 inches) between the wall and the underside of the screw head.
 - The maximum distance from the wall to the top of the screw head is 7.6 mm (.3 in).



- 11** Remove the two plastic feet, nearest to the LED panel, from the bottom of the router to uncover the keyholes.
- 12** Place the router so the keyholes are above the mounting screws.
- 13** Slide the router down until it stops against the top of the keyhole opening.
- 14** Follow the installation procedures for connecting and configuring the router.

Electrical Connection

Your router does not have an On/Off power switch and therefore will only be powered on by plugging in the power adapter



- 1** Connect the power adapter to the router's **Power** port, found on the back of the router.
- 2** Plug the power adapter into a grounded and surge-protected power outlet. The Power LED on the front panel lights green when connected properly.

Establishing Your First Connection to the WR850

Once the WR850 is placed, you can now establish your first PC connection to the WR850. There are three ways to choose from to accomplish this:

- (1) If your first connection will be a wired connection (i.e., an Ethernet cable will connect the PC and the WR850), you can follow the step-by-step easy install process with the included *WR850 Installation Wizard CD-ROM*. **[recommended]**
- (2) If your first connection will be a wired connection, but you do not wish to use the *WR850 Installation Wizard CD-ROM*, you can manually install this first wired connection.
- (3) If your first connection will be a wireless connection, you can manually install this first wireless connection.

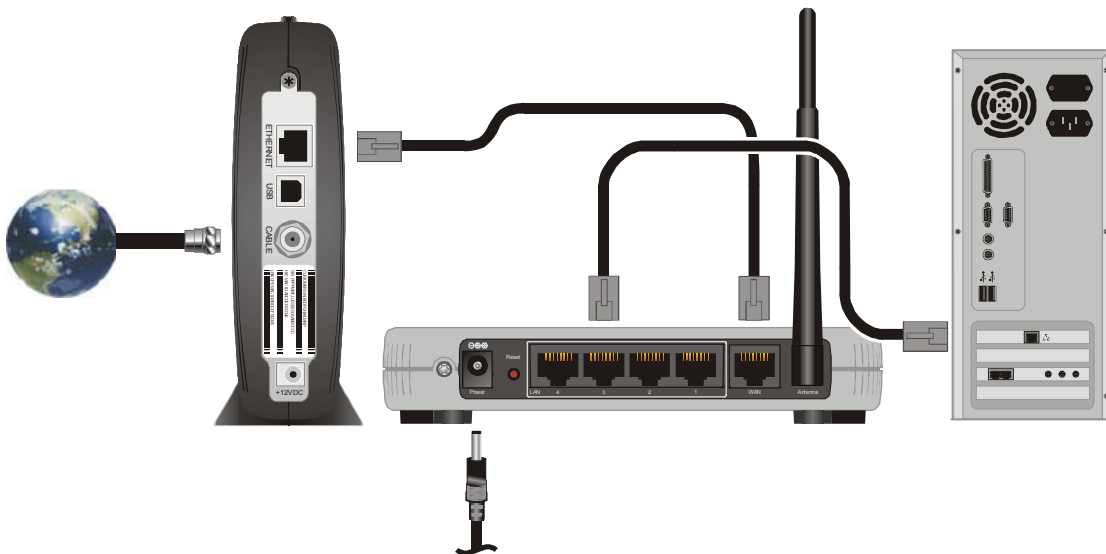
Easy Install Process

Run the Installation Wizard program from the supplied CD-ROM to quickly set up your network. Once your network is up and running, for advanced configuration, see Section 3: Configuration.

The Installation Wizard will automatically run once you place the CD-ROM in your PC's CD-ROM drive. It will confirm that the antenna and electrical connections have been made, and then lead you step-by-step through setting up your WR850 in a typical configuration as a wired/wireless router.

Manual Install – Wired Connection

If you are manually connecting your PC with an Ethernet cable to the router, your PC must be installed first with an Ethernet adapter. *You need two Ethernet cables for this procedure, one to connect the router to the modem and one to connect a PC to the router.*



- 1 If you are currently running broadband to a single computer: Unplug the Ethernet cable that runs between your modem and PC from the back of your PC and plug it into the port labeled **WAN** on the back of your router.

If you are not running broadband to a single computer: Connect an Ethernet cable to the **WAN** port on your router.

- 2 Connect the other end of the same cable to your cable or DSL modem. You have now connected the router to the modem. It will be necessary to restart your cable or DSL modem after making this connection.
- 3 To connect the PC to the router, use a second Ethernet cable and connect it to the Ethernet port on your PC.
- 4 Connect the other end of the same cable into one of the **LAN** ports on your router. You have now connected your PC to the router.
- 5 Your PC's Ethernet adapter may need to be configured to work with the WR850.

By default, the WR850 has a LAN IP Address of 192.168.10.1, and dynamically assigns an IP Address to connected devices. The PC will not communicate properly with the WR850 if the Ethernet adapter is not configured either:

- (a) to accept a dynamic IP Address, or
- (b) with a compatible static IP Address (i.e., 192.168.10.x, where x is a number between 2 and 254).

To make any necessary adjustments to your PC's Ethernet Adapter, you can follow the instructions in this section under *Configuring Computers to Communicate with the WR850*.

NOTE: You can make wired connections between the WR850 and other devices by repeating Steps 3, 4, and 5 with each of those devices.

- 6 Once the PC is communicating with the WR850, you can proceed to *Section 3: Configuration* to access the built-in Web-based Configuration Utility and configure the WR850:
 - *For a typical WR850 configuration as a wired/wireless router*, review and adjust as necessary only those configuration options designated as “commonly used” or “recommended”. These fields are labeled with **white** letters.
 - *For advanced WR850 configuration*, review and adjust any and all configuration options as desired. Field codes requiring more advanced knowledge to configure are labeled with **black** letters.

Manual Install – Wireless Connection

WARNING!

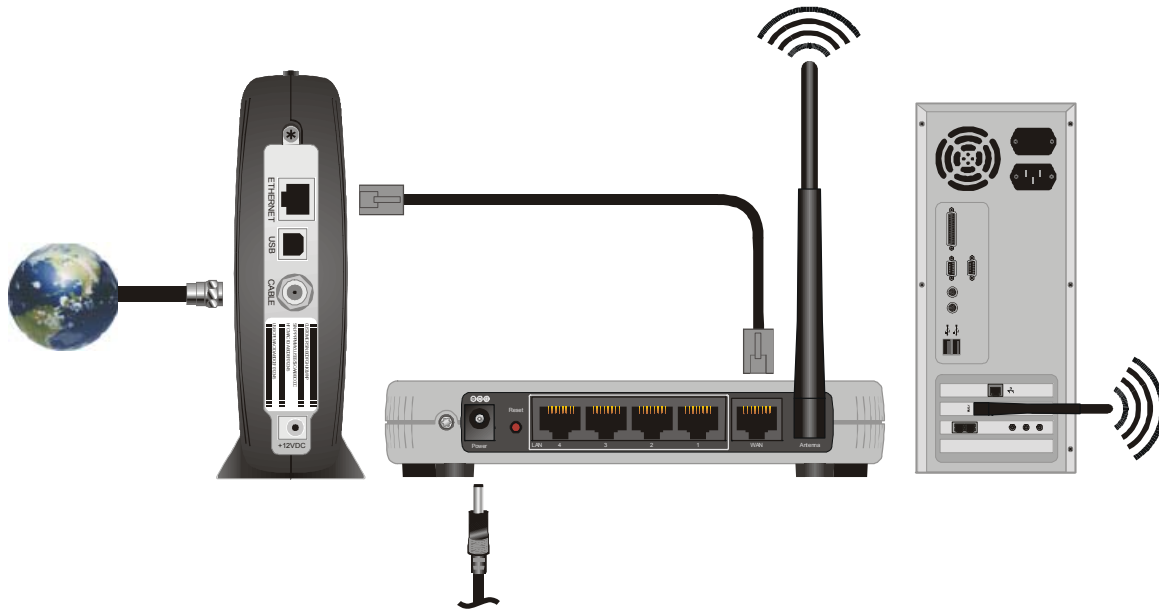


When first configuring your router, it is recommended that you have an Ethernet cable connected to the router. Performing the INITIAL configuration using a wireless connection is not secure and is not recommended.

After you have finished the initial configuration of the router, your connection will be secure and you can safely use either a wired or wireless connection.

If you are connecting your client wirelessly to the router, you can use the Motorola WPCI810G or WPCI810GP, a wireless PCI adapter for your desktop PC. If you have a laptop, the Motorola WN825G or WN825GP wireless PC card adapter provides access. A Motorola WU830G wireless USB adapter can also provide access for desktops or laptops.

The WPCI810G, WN825G, and WU830G support the Windows® 98SE, Windows Me®, Windows® 2000, and Windows XP™ operating systems. The WPCI810GP and WN825GP support Windows 2000 and XP only. None of these adapters support Windows® 95, Windows® 98, or Windows NT®.



- 1 If you are currently running broadband to a single computer, unplug the Ethernet cable that runs between your modem and PC from the back of your PC and plug it into the port labeled **WAN** on the back of your router.

If you are not running broadband to a single computer, connect an Ethernet cable to the **WAN** port on your router.

- 2 Connect the other end of the same cable to your cable or DSL modem. You have now connected the router to the modem. It will be necessary to restart your cable or DSL modem after making this connection.

- 3 Your PC's wireless adapter may need to be configured to work with the WR850.

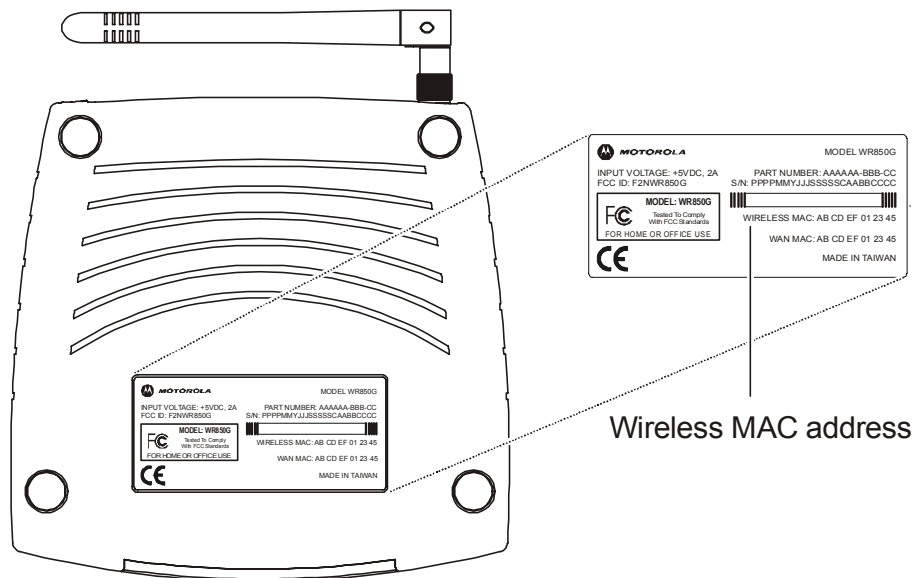
By default, the WR850 has a LAN IP Address of 192.168.10.1, and dynamically assigns an IP Address to connected devices. The PC will not communicate properly with the WR850 if the wireless adapter is not configured either:

- (a) to accept a dynamic IP Address, or
- (b) with a compatible static IP Address (i.e., 192.168.10.x, where x is a number between 2 and 254).

To make any necessary adjustments to your PC's wireless adapter, you can follow the instructions in this section under *Configuring Computers to Communicate with the WR850*.

- 4 To connect the PC to the WR850 through a wireless connection, use your PC's wireless adapter utility to verify:

- (a) the selection of the SSID (Service Set Identifier) of the WR850, which by default is set to **motorolaABCDEF012345**, where the final 12 characters represent the WR850's Wireless MAC address (see the image below to identify the WR850 Wireless MAC address from the product label),
- (b) that authentication is set to Open, since the WR850 by default has no wireless authentication enabled, and
- (c) that no encryption is enabled, since the WR850 by default has no wireless encryption enabled.



Refer to your wireless adapter's documentation for instructions on how to review and adjust these settings.

NOTE: You can make wireless connections between the WR850 and other devices by repeating Steps 3 and 4 with each of those devices, but it is recommended to wait until after securing your wireless network to do so.

5 Once the PC is communicating with the WR850, you can proceed to *Section 3: Configuration* to access the built-in Web-based Configuration Utility and configure the WR850:

- *For a typical WR850 configuration as a wired/wireless router*, review and adjust as necessary only those configuration options designated as “commonly used” or “recommended”. These fields are labeled with **white** letters.
- *For advanced WR850 configuration*, review and adjust any and all configuration options as desired. Field codes requiring more advanced knowledge to configure are labeled with **black** letters.

In either case, it is recommended that you first use the Web-based Configuration Utility to establish security measures on your wireless network, and re-connect securely to the WR850, prior to making any other changes to the WR850.

Configuring Computers to Communicate with the WR850

Each computer that will be part of your network needs to communicate with the router. To do this, you may need to configure each PC's network settings to automatically obtain an IP address.

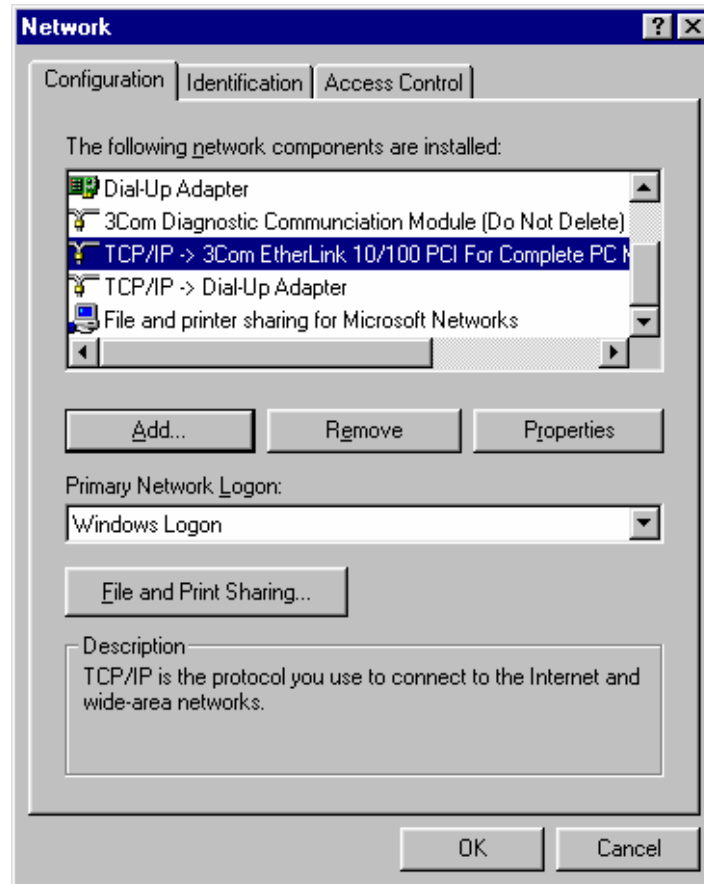
This section includes information on configuring computers with the following operating systems:

- Windows® 98SE
- Windows Me®
- Windows® 2000
- Windows XP™

Determine the operating system for each computer you will include in your wireless network and follow the steps to configure the network settings for that PC.

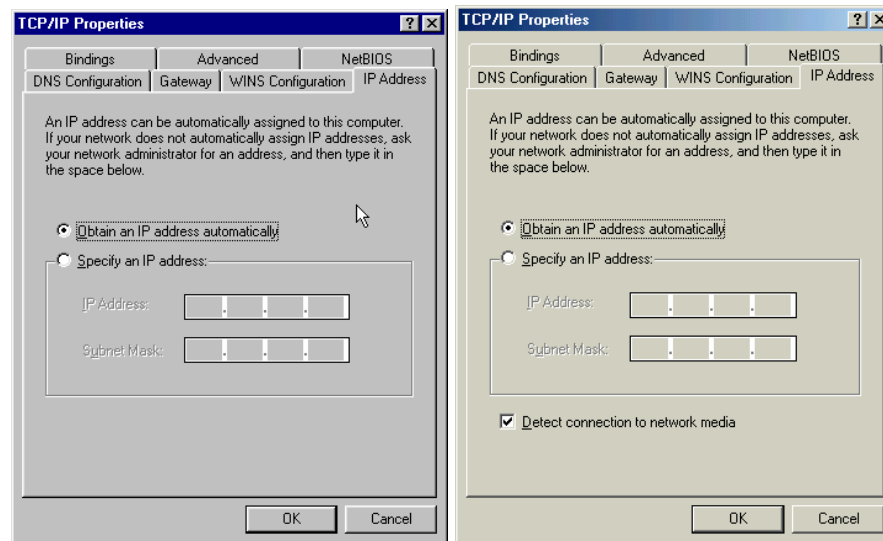
Configuring Windows 98SE and ME

- 1 Click **Start**.
- 2 Select **Settings > Control Panel**.
- 3 Double-click **Network**. The Network window is displayed.



- 4 On the Configuration tab, select the **TCP/IP** line the for the appropriate wired or wireless Ethernet adapter on your PC. There may be multiple adapters installed – choose only the one that is configured for your adapter. In the example above, a 3Com Ethernet adapter card is installed and is the appropriate choice.

- 5 Click **Properties**. The TCP/IP Properties window is displayed.



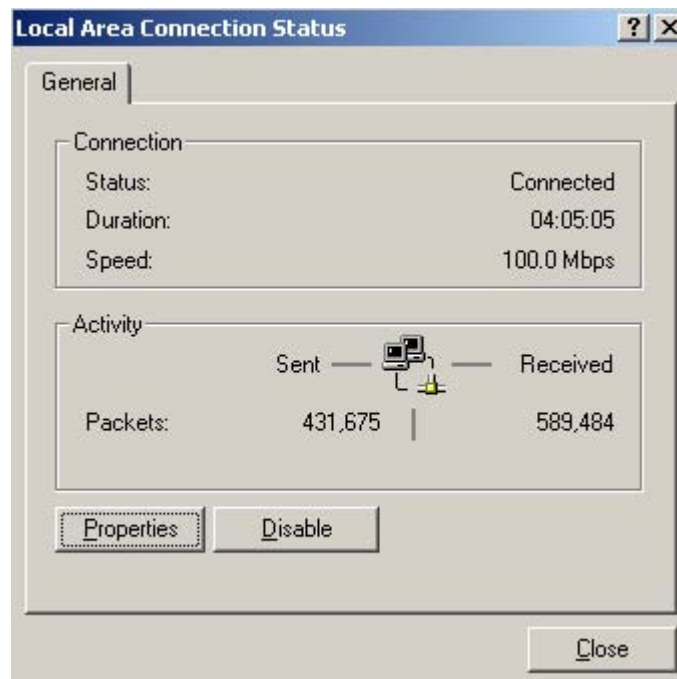
Windows 98SE

Windows ME

- 6 Click the **IP Address** tab.
- 7 Select ***Obtain an IP address automatically***.
- 8 Click **OK**.
- 9 Click the **Gateway** tab and confirm that the *Installed Gateway* field is blank.
- 10 Click **OK** twice. Windows may ask for the Windows Installation disk. First check to see if the installation files are installed at c:\windows\options\cabs. Otherwise, load your Windows CD and follow the prompts.
- 11 Restart your computer to save your settings.

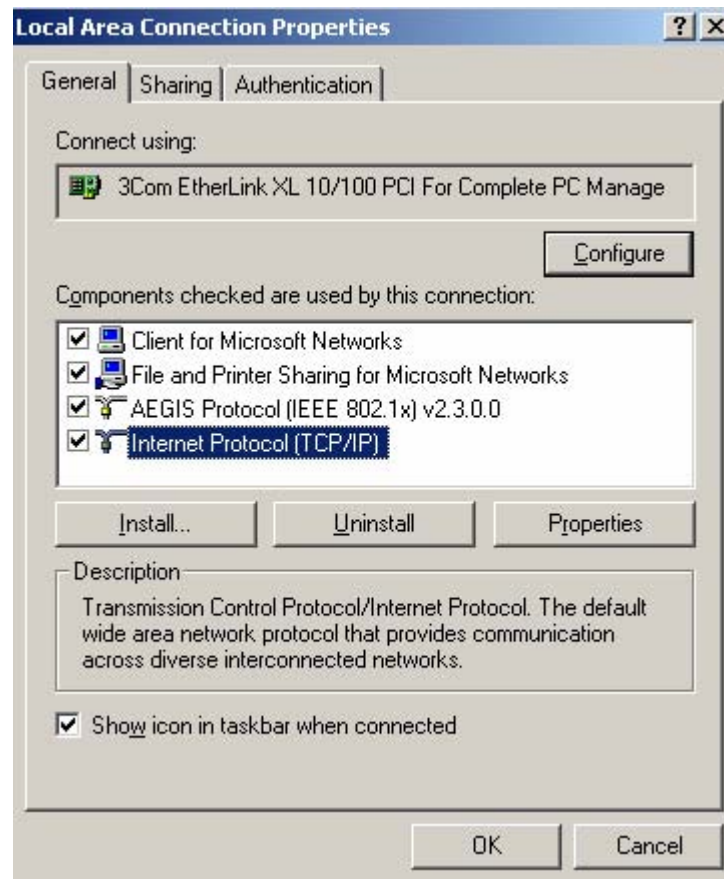
Configuring Windows 2000

- 1 Click **Start**.
- 2 Select **Settings**.
- 3 Select **Control Panel**.
- 4 Double-click **Network and Dial-Up Connections**.
- 5 Double-click the **Local Area Connection** appropriate for your wired or wireless Ethernet adapter.



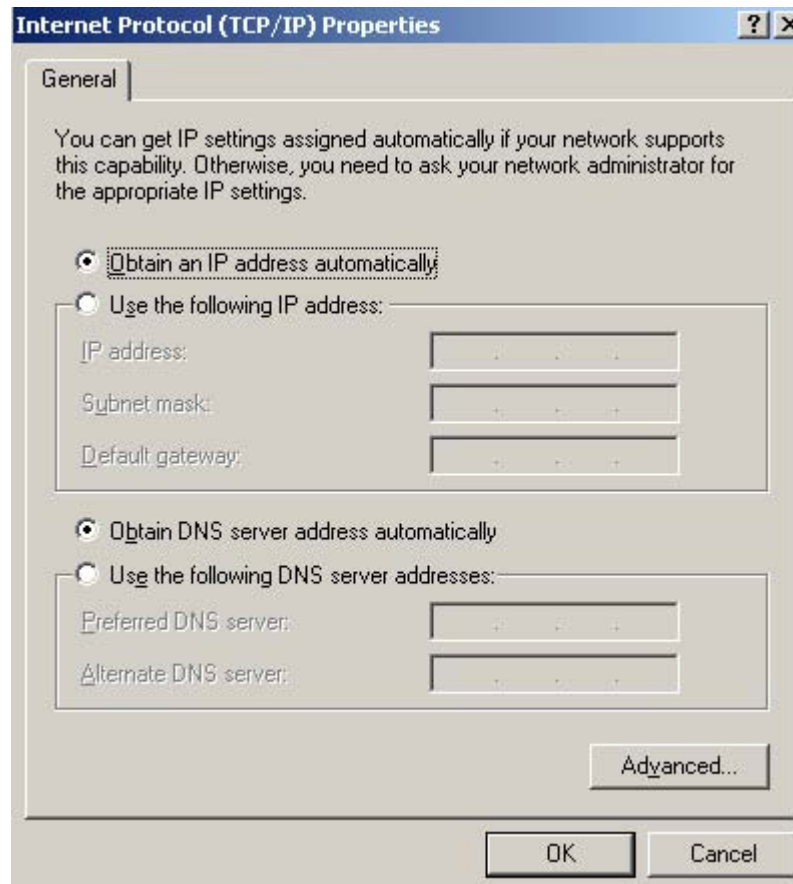
- 6 Click **Properties**.

The Local Area Properties window is displayed.



- 7 Ensure the box next to **Internet Protocol (TCP/IP)** is selected.
- 8 Click to highlight **Internet Protocol (TCP/IP)** and click **Properties**.

The Internet Protocol (TCP/IP) Properties window is displayed.

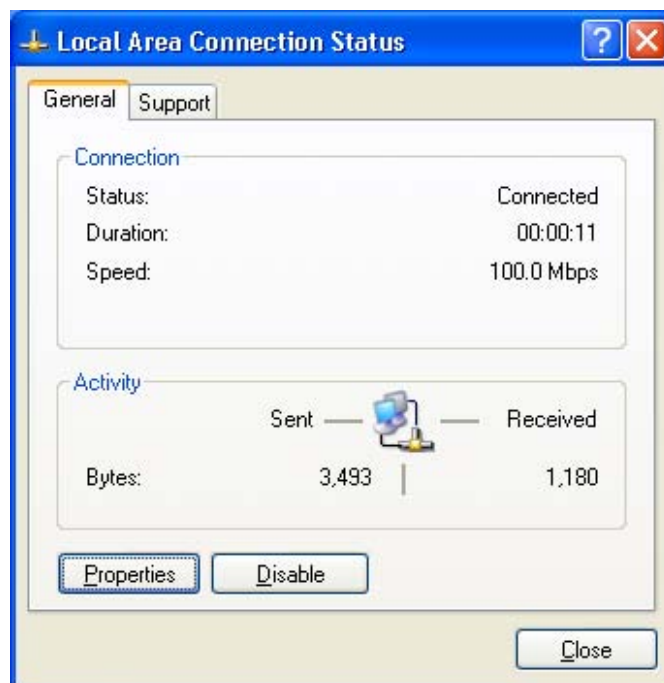


- 9 Select **Obtain an IP address automatically**. Click **OK** twice to exit and save your settings.
- 10 Restart your computer to save your settings.

Configuring Windows XP

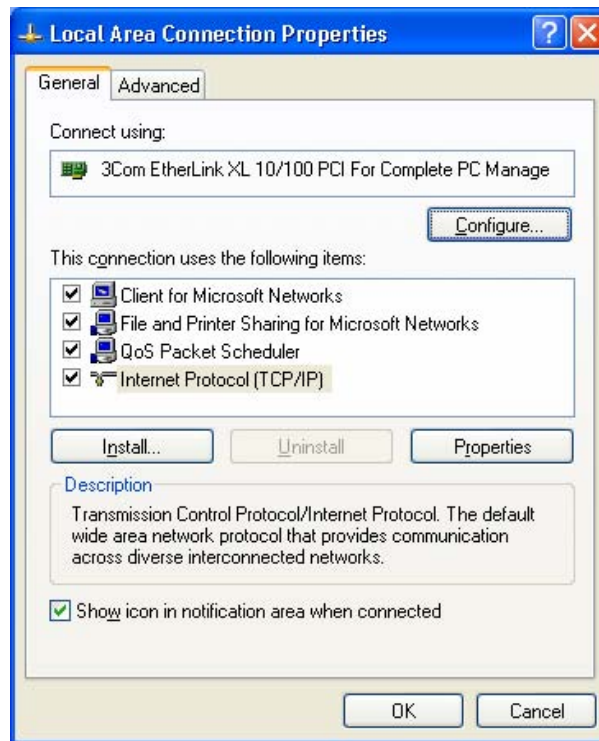
This configuration assumes you have retained the default interface for Windows XP. If you are running the 'Classic' interface, please follow the instructions for Windows 2000.

- 1 Click **Start**.
- 2 Select **Settings**.
- 3 Select **Control Panel**.
- 4 Double-click **Network and Dial-Up Connections**.
- 5 Double-click the **Local Area Connection** appropriate for your wired or wireless Ethernet adapter.



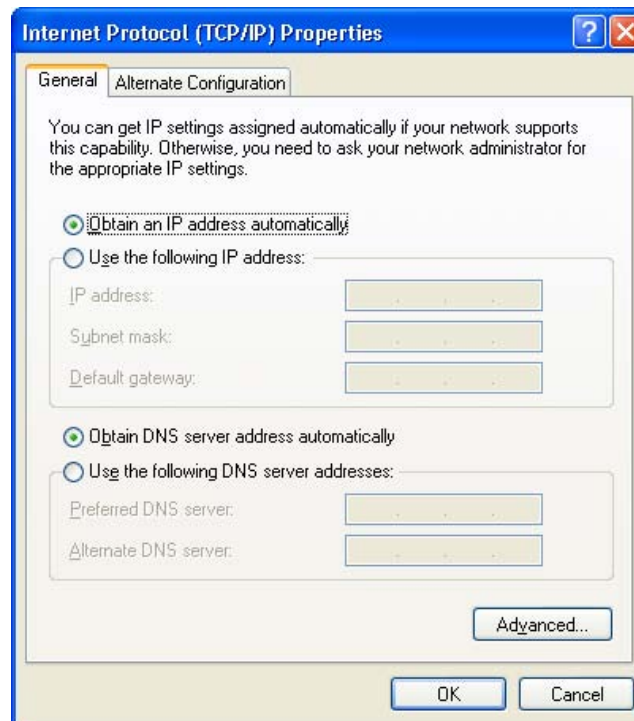
- 6 Click **Properties**.

The Local Area Properties window is displayed.



- 7 Ensure the box next to *Internet Protocol (TCP/IP)* is selected.
- 8 Click to highlight **Internet Protocol (TCP/IP)** and click **Properties**.

The Internet Protocol (TCP/IP) Properties window is displayed.



- 9 Click **Obtain an IP address automatically**. Click **OK** twice to exit and save your settings.

Section 3: Configuration

This section describes how to use the Web-based Configuration Utility built into your WR850 Wireless Broadband Router. This utility allows you to customize the WR850 to meet your specific needs.

The Web-based Configuration Utility provides several pages of configuration options. These configuration options are factory set to default values, based on the typical use of the WR850 as a wired/wireless router. When you login to the utility for the first time, you will find all options set to these factory defaults, unless you have already made changes by running the WR850 Installation Wizard CD-ROM.

In fact, if you have already used the WR850 Installation Wizard CD-ROM to initially set up your router, in many cases you will not need to adjust any other configuration options.

Where adjustments of configuration options are required, additional online help is provided through “rollover” descriptions. While using the Web-based Configuration Utility, as you roll your mouse cursor over the name of any configuration option, a brief description of that option will be displayed.

NOTE: The screenshots shown are intended for reference only; your version of firmware may differ slightly.

Accessing the Web-Based Configuration Utility

Logging In

- 1 Once the router is connected, open your web browser. In the URL field enter **http://192.168.10.1** (the router's default IP address). Press the **Enter** key.



The login window will appear (the WR850GP login window is shown in the example below):

A screenshot of a login window titled 'Enter Network Password'. The window has a blue title bar with a help icon and a close button. Inside, there is a key icon and the text 'Please type your user name and password.' Below this, the 'Site:' is '192.168.10.1' and the 'Realm' is 'Motorola Wireless Broadband Router WR850GP'. There are two input fields: 'User Name' with 'admin' entered, and 'Password' with 'xxxxxxx' entered. At the bottom, there is a checkbox labeled 'Save this password in your password list' which is unchecked. There are 'OK' and 'Cancel' buttons at the bottom right.

- 2 Enter the **User Name**. The default factory setting is *admin*.
- 3 Enter the **Password**. The default factory setting is *motorola*.
Once you have logged in, for security reasons you should change the User ID and Password. See below.
- 4 Click **OK** to enter the Web-based Configuration Utility.
The BASIC configuration page will appear when entering the Web-based Configuration Utility.

Overview of Configuration Pages

Navigation Between Pages

The Web-based Configuration Utility is made up of nine configuration pages, each with configuration options tied to different functions of the WR850. A “selection bar,” listing all of these configuration pages, appears at the top of each configuration page.

Figure 3-2 Configuration Page Selection Bar



You can access any page by moving the cursor over a specific configuration page title in the selection bar, and clicking on the page title.

These configuration pages are as follows:

- **BASIC:** This page allows you to configure basic access and control features of your WR850.
- **LAN (LOCAL AREA NETWORK):** This page allows you to configure your WR850 to support connections to devices within your local home or small office network.
- **WAN (WIDE AREA NETWORK):** This page allows you to configure your WR850 to support connections to broadband services.
- **STATUS:** This page displays information about the status of your WR850.
- **FILTERS:** This page allows you to configure two types of filters, allowing you to block undesired use of your broadband connection. One potential use of these filters is to set parental controls on the use of the Internet.
- **ROUTING:** This page allows you to configure port forwarding and triggering rules, as needed to allow specific clients on your local network to run and share certain programs that use the Internet.
- **WIRELESS:** This page allows you to configure your wireless network.
- **SECURITY:** This page allows you to configure security features to protect information shared over wireless connections.
- **FIRMWARE:** This page allows you to upgrade the firmware of your WR850.

*On each configuration page, the most commonly used configuration options are highlighted in **white** for easy reference. What follows are page-by-page descriptions of the configuration options available.*

The BASIC Configuration Page

This page allows you to configure basic access and control features of your WR850. It is the first page you see when entering the Web-based Configuration Utility.

Figure 3-1 BASIC Page

MOTOROLA WR850GP

Basic LAN WAN Status Filters Routing Wireless Security Firmware

BASIC
This page allows you to configure basic access and control features of your router/access point.

Notes:
[1] Fields labeled in **black** are typically customized by advanced users.
[2] When you click **Apply** to make **Operation Mode** change on this BASIC page, or click **Restore Factory Configuration**, your router/access point will restart to apply the changes.

Configuration Login Username: admin
Configuration Login Password: *****
Remote Login Port:
Operation Mode: Router
Firewall: Enabled
Universal Plug and Play (UPnP): Enabled
Local Time: Thu Jan 1 00:00:12 1970
Time Zone: (GMT-05:00) Eastern Time (USA & Canada)
Auto Adjust for Daylight Saving Time: Enabled
Internet Time Server Addresses: 216.211.136.180
207.104.100.201
Event Log Destination Address:
Connection Logging: Disabled

Apply Cancel Restart Restore Factory Configuration

BASIC Page – Commonly Used Configuration Options

The following configuration options are highlighted in **white** on the BASIC Page for easy reference. These fields are the most commonly used or adjusted in supporting typical uses of the WR850 as a wired/wireless router.

The rest of the configuration options are provided primarily for advanced users.

Field	Description																																				
Configuration Login Username:	Sets your user name to access this Web-based Configuration Utility. FACTORY DEFAULT: admin																																				
Configuration Login Password:	Sets your password to access this Web-based Configuration Utility. FACTORY DEFAULT: motorola																																				
<p>NOTE: Once you have logged in, for security reasons you should change the default User Name and Password. If necessary, the default settings can be reset, either by clicking the Restore Factory Configuration button at the bottom of the BASIC Page (which will reset all options to factory defaults) or by using the Reset button on the back of the WR850 (which, as referenced in Section 1 of this User Guide, will reset only a select number of options).</p> <p>If you wish, you can disable access control by leaving both the Configuration Login Username and Configuration Login Password blank, but this is <u>not</u> recommended.</p>																																					
Time Zone:	Sets the time zone for your location from among the following:																																				
	<table><tr><td>Kwajalein</td><td>Atlantic Time (Canada) Brazil West</td><td>Armenia</td></tr><tr><td>Midway Island, Samoa</td><td>Guyana</td><td>Pakistan, Russia</td></tr><tr><td>Hawaii</td><td>Brazil East, Greenland</td><td>Bangladesh, Russia</td></tr><tr><td>Alaska</td><td>Mid-Atlantic</td><td>Thailand, Russia</td></tr><tr><td>Pacific Time (USA, Canada)</td><td>Azores</td><td>China, Hong Kong, Australia Western</td></tr><tr><td>Arizona</td><td>Gambia, Liberia, Morocco</td><td>Singapore, Taiwan, Russia</td></tr><tr><td>Mountain Time (USA, Canada)</td><td>England</td><td>Japan, Korea</td></tr><tr><td>Mexico</td><td>Tunisia</td><td>Guam, Russia</td></tr><tr><td>Central Time (USA, Canada)</td><td>France, Germany, Sweden, Finland</td><td>Australia</td></tr><tr><td>Indiana East, Colombia, Panama</td><td>South Africa</td><td>Solomon Islands</td></tr><tr><td>Eastern Time (USA, Canada)</td><td>Greece, Ukraine, Romania, Turkey</td><td>Fiji</td></tr><tr><td>Bolivia, Venezuela</td><td>Iraq, Jordan, Kuwait</td><td>New Zealand</td></tr></table>	Kwajalein	Atlantic Time (Canada) Brazil West	Armenia	Midway Island, Samoa	Guyana	Pakistan, Russia	Hawaii	Brazil East, Greenland	Bangladesh, Russia	Alaska	Mid-Atlantic	Thailand, Russia	Pacific Time (USA, Canada)	Azores	China, Hong Kong, Australia Western	Arizona	Gambia, Liberia, Morocco	Singapore, Taiwan, Russia	Mountain Time (USA, Canada)	England	Japan, Korea	Mexico	Tunisia	Guam, Russia	Central Time (USA, Canada)	France, Germany, Sweden, Finland	Australia	Indiana East, Colombia, Panama	South Africa	Solomon Islands	Eastern Time (USA, Canada)	Greece, Ukraine, Romania, Turkey	Fiji	Bolivia, Venezuela	Iraq, Jordan, Kuwait	New Zealand
	Kwajalein	Atlantic Time (Canada) Brazil West	Armenia																																		
	Midway Island, Samoa	Guyana	Pakistan, Russia																																		
	Hawaii	Brazil East, Greenland	Bangladesh, Russia																																		
	Alaska	Mid-Atlantic	Thailand, Russia																																		
	Pacific Time (USA, Canada)	Azores	China, Hong Kong, Australia Western																																		
	Arizona	Gambia, Liberia, Morocco	Singapore, Taiwan, Russia																																		
	Mountain Time (USA, Canada)	England	Japan, Korea																																		
	Mexico	Tunisia	Guam, Russia																																		
	Central Time (USA, Canada)	France, Germany, Sweden, Finland	Australia																																		
	Indiana East, Colombia, Panama	South Africa	Solomon Islands																																		
	Eastern Time (USA, Canada)	Greece, Ukraine, Romania, Turkey	Fiji																																		
Bolivia, Venezuela	Iraq, Jordan, Kuwait	New Zealand																																			
FACTORY DEFAULT: Eastern Time (USA & Canada)																																					

BASIC Page – All Configuration Options

Options related to: CONTROLLING ACCESS TO THE CONFIGURATION UTILITY

Configuration Login Username:

Configuration Login Password:

Remote Login Port:

Field	Description
Configuration Login Username:	Sets your user name to access this Web-based Configuration Utility. FACTORY DEFAULT: admin
Configuration Login Password:	Sets your password to access this Web-based Configuration Utility. FACTORY DEFAULT: motorola
<p>NOTE: Once you have logged in, for security reasons you should change the default User Name and Password. If necessary, the default settings can be reset, either by clicking the Restore Factory Configuration button at the bottom of the BASIC Page (which will reset all options to factory defaults), or by using the Reset button on the back of the WR850 (which, as referenced in Section 1 of this User Guide, will reset only a select number of options).</p> <p>If you wish, you can disable access control by leaving both the Configuration Login Username and Configuration Login Password blank, but this is <u>not</u> recommended.</p>	
Remote Login Port: (ADVANCED)	Enables access to the Web-based Configuration Utility while away from your home or office, through your broadband connection. An HTTP port (such as 8080) must be provided to enable remote access. Leave this field blank to disable remote access. FACTORY DEFAULT: (blank)

Options related to: ENABLING PRIMARY ROUTER FUNCTIONS

Operation Mode:

Firewall:

Universal Plug and Play (UPnP):

Field	Description
Operation Mode: (ADVANCED)	<p>Enables the primary router functions of the WR850. These router functions include:</p> <ul style="list-style-type: none"> Routing data in your local network using IP addresses of the connected devices, allowing the IP address for your broadband connection to be shared among those devices. <p>This is called <i>Network Address Translation (NAT)</i>.</p> <p style="text-align: right;">(continued on next page)</p>

Field	Description
Operation Mode: (continued)	<ul style="list-style-type: none"> Dynamically assigning IP addresses to devices on your local network, simplifying network set-up, using the Dynamic Host Configuration Protocol (DHCP). This is the WR850's built-in local area network <i>DHCP server</i> (which is configured on the LAN Page). Routing and/or filtering data based on the protocol used and/or its content, protecting your broadband connection and your local network from undesired access. This is the WR850's built-in <i>firewall</i> (which can be configured with specific filters on the FILTERS Page, and with specific routing "rules" on the ROUTING Page). <p>If all of these router functions are disabled, the WR850 simply operates as a combination of a wireless access point and a wired 5-port Ethernet switch (the physical port labeled "WAN" becomes the fifth "switched" port, along with the four "LAN" ports).</p> <p>With router functions disabled, all WR850 configuration options that use the <u>IP addresses</u> of local network devices are disabled (with any entries into those fields ignored). However, all WR850 configuration options that use <u>Media Access Control (MAC) addresses</u> of local network devices – physical addresses uniquely assigned by manufacturers to any network device -- are still available.</p> <ul style="list-style-type: none"> Selecting Router enables router functions. Selecting Access Point disables router functions. <p>NOTE: If you wish to enable some router functions and not all, select Router and then disable specific router functions via their respective configuration options that follow.</p> <p>For example, if you wish to use the firewall but have no need for the DHCP server, select Router here and then disable DHCP Server on the LAN Page.</p> <p>FACTORY DEFAULT: Router</p>
Firewall: (ADVANCED)	<p>Enables the built-in firewall, to protect your router and local network from unauthorized access from the Internet.</p> <ul style="list-style-type: none"> Selecting Enabled engages the built-in firewall. Selecting Disabled disengages the built-in firewall. <p>NOTE: It is recommended that the firewall be disabled only if you are using alternative firewall protection software.</p> <p>NOTE: Firewall is greyed out to Disabled if Operation Mode (above) is set to Access Point.</p> <p>FACTORY DEFAULT: Enabled</p>

Field	Description
UPnP: (ADVANCED)	<p>Enables Universal Plug and Play (UPnP) operation, a feature required by some software programs to automatically configure your router for compatibility.</p> <ul style="list-style-type: none"> Selecting Enabled allows these software programs to automatically manage compatibility with the router, without additional user configuration. Selecting Disabled does not allow these software programs to automatically manage compatibility with the router. <p>NOTE: <i>UPnP requires router functions to be enabled. This setting will only be used if Operation Mode (above) is set to Router.</i></p> <p>FACTORY DEFAULT: Enabled</p>

Options related to: ENABLING TIME-RELATED FUNCTIONS

Local Time: Thu Jan 1 00:00:12 1970

Time Zone: (GMT-05:00) Eastern Time (USA & Canada) ▼

Auto Adjust for Daylight Saving Time: Enabled ▼

Internet Time Server Addresses:

216.211.136.180

207.104.100.201

Field	Description
Local Time (DISPLAY ONLY)	Shows the day, month, year and local time (in that order), as maintained by the WR850.
Time Zone:	<p>Sets the time zone for your location. See drop-down listing for available time zones.</p> <p>FACTORY DEFAULT: Eastern Time (USA & Canada)</p>
Auto Adjust for Daylight Saving Time	<p>Enables automatic adjustment of local time for Daylight Saving Time. Select Disabled if Daylight Saving Time is not observed in your area.</p> <p>FACTORY DEFAULT: Enabled</p>

Internet Time Server Addresses: (ADVANCED)	<p>The WR850 can use an Internet time server to maintain the integrity of time-dependent router functions (logging, filtering, etc.). Motorola sponsors two Internet time servers; their IP addresses are listed in the first two address fields, making them the first two time servers used.</p> <p>You may add one IP address for an additional Internet time server. This would serve as a back-up resource, if for any reason the Motorola servers are temporarily unavailable.</p> <p>FACTORY DEFAULT: Motorola time servers are listed in fields 1 and 2; field 3 is blank.</p>
---	--

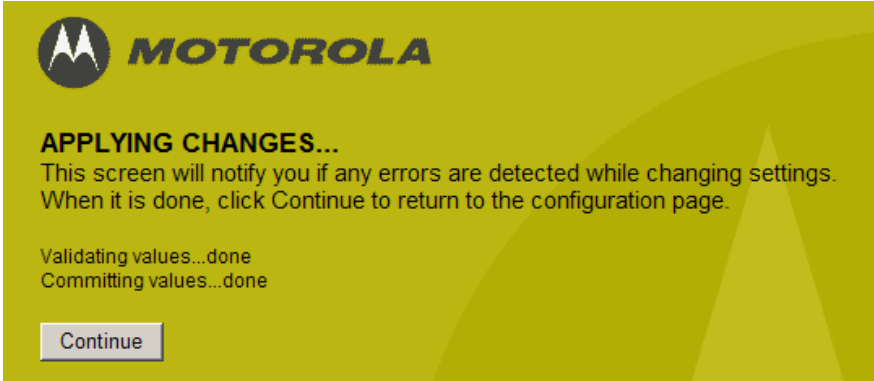
Options related to: LOGGING WR850 ACTIVITY

Event Log Destination Address:	<input type="text"/>
Connection Logging:	Disabled <input type="button" value="v"/>

Field	Description
Event Log Destination Address: (ADVANCED)	<p>Sets an IP address as the destination for the posting of router logs. Logs are posted in a “syslog” format; you can read them using a Syslog Daemon (e.g., the Kiwi Syslog Daemon, etc.), which can often be found offered as freeware on the Internet.</p> <p>Leave this field blank to set the STATUS Page (within this Web-based Configuration Utility) as the only destination for router logs.</p> <p>FACTORY DEFAULT: (blank)</p>
Connection Logging: (ADVANCED)	<p>Sets the types of router connections to be logged.</p> <ul style="list-style-type: none"> • Selecting Accepted will only log accepted connections. • Selecting Denied will only log denied connections. • Selecting Disabled will log neither accepted nor denied connections. • Selecting Both will log both accepted and denied connections. <p>FACTORY DEFAULT: Disabled</p>

BASIC Page Action Buttons

At the bottom of the BASIC Page, you will see four click-able buttons to process any desired changes to the configuration options.

Button	Purpose
Apply	<p>This button allows you to apply the settings you have selected for BASIC Page configuration options.</p> <p>When you click the Apply button, you will see an “Applying Changes” page that shows the status of validating and committing the new selections that have been made.</p>  <p>If no errors were made in the new selections, the prior selections (including any default settings) will be overridden with your new selections. If errors were made in the new selections, you can return to the BASIC Page to correct and re-apply them.</p> <p><u>NOTE:</u> <i>Applying changes on the BASIC Page will reboot your WR850. During a reboot, you may temporarily lose your connection to the Web-based Configuration Utility.</i></p>
Cancel	<p>Cancels all changes you have made on the BASIC Page, reverting the page to its previously saved configuration.</p> <p>Any new selections will be deleted and not be applied.</p>
Restart	<p>Restarts your WR850. This can be used to reset WR850 logs and refresh information.</p>
Restore Factory Configuration	<p>This button resets all configuration options to their original factory default settings.</p> <p><u>NOTE:</u> <i>This button will reset configuration options on all pages to defaults, not just the options on the BASIC Page.</i></p>

The LAN (Local Area Network) Configuration Page

This page allows you to configure your WR850 to support connections to devices within your local home or small office network, or LAN. This can include devices connected via the WR850 wired LAN ports, or via the built-in wireless access point.

Figure 3-4 Local Area Network (LAN) Page

MOTOROLA WR850GP

Basic **LAN** WAN Status Filters Routing Wireless Security Firmware

LOCAL AREA NETWORK (LAN)
This page allows you to configure your router/access point to support connections to devices within your local home or small office network.

MAC Address: 00:0C:E5:51:A6:D1

Protocol: Static

IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.1

DHCP Server: Enabled

DHCP Starting IP Address: 192.168.10.2

DHCP Ending IP Address: 192.168.10.254

DHCP Lease Time: 86400

Active DHCP Leases:

Hostname	MAC Address	IP Address	Expires In
MG102C-01	00:0F:66:1D:F5:99	192.168.10.2	23 hours, 47 minutes, 56 seconds

Spanning Tree Protocol: Enabled

Static Routes:

IP Address	Subnet Mask	Gateway	Metric

Apply Cancel

LAN Page – Commonly Used Configuration Options

None of the configuration options on the LAN Page typically require any adjustment from factory defaults, to support most typical uses of the WR850 as a wired/wireless router.

Therefore, none of the configuration options on the LAN Page are highlighted in **white**. LAN Page configuration options are provided primarily for advanced users.

LAN Page – All Configuration Options

Options related to: SELECTING THE WR850 LOCAL AREA NETWORK PROTOCOL

MAC Address: 00:0C:E5:51:A6:D1

Protocol: Static

IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.1

Field	Description
MAC Address: (DISPLAY ONLY)	Shows the Media Access Control (MAC) address of the WR850 LAN connections. This is the physical address of these LAN connections.
Protocol: (ADVANCED)	<p>Sets the method by which an IP address is assigned to the WR850's LAN connections.</p> <ul style="list-style-type: none"> Selecting Static requires that a unique and permanent IP address be assigned, in the <i>IP Address</i> field just below. Selecting DHCP assumes that a Dynamic Host Configuration Protocol server is on your LAN and can assign the WR850 an IP address. You will want to disable the WR850 DHCP server below. <p>NOTE: If Operation Mode on the <i>BASIC Page</i> is set to Router, this field is set to Static (and you will not be able to select DHCP).</p> <p>FACTORY DEFAULT: Static</p>
IP Address: (ADVANCED)	<p>Sets the IP address for the WR850 LAN connections, when the <i>Protocol</i> field is set to Static.</p> <p>NOTE: Changing this IP Address will change the address at which you access the Web-based Configuration Utility.</p> <p>NOTE: Changing this IP Address should be coordinated with the IP addresses you assign to devices that will connect to the WR850.</p> <p>NOTE: If Protocol (above) is set to DHCP, this field will be greyed out, and any data entered will not be used.</p> <p>FACTORY DEFAULT: 192.168.10.1</p>
Subnet Mask: (ADVANCED)	<p>Sets the subnet mask for the WR850 LAN connections, when the <i>Protocol</i> field is set to Static. The subnet mask is used to divide your LAN into multiple "subnets."</p> <p>NOTE: If Protocol (above) is set to DHCP, this field will be greyed out, and any data entered will not be used.</p> <p>FACTORY DEFAULT: 255.255.255.0</p>

Field	Description
Default Gateway: (ADVANCED)	Sets the IP address of the default gateway for the WR850 connections, when the <i>Protocol</i> field is set to Static. The default gateway is set by default to be the WR850 (i.e., the factory default IP address matches that of the WR850). NOTE: If Protocol (above) is set to DHCP , this field will be greyed out, and any data entered will not be used. FACTORY DEFAULT: 192.168.10.1

Options related to: ENABLING THE WR850 BUILT-IN DHCP SERVER

DHCP Server:

DHCP Starting IP Address:

DHCP Ending IP Address:

DHCP Lease Time:

Active DHCP Leases:

Hostname	MAC Address	IP Address	Expires In
MG102C-01	00:0F:66:1D:F5:99	192.168.10.2	23 hours, 47 minutes, 56 seconds

Field	Description
DHCP Server: (ADVANCED)	Sets the method by which IP addresses are assigned to devices that interface with the WR850 via the LAN connections (or “clients”). <ul style="list-style-type: none"> Selecting Enabled engages the Dynamic Host Configuration Protocol (DHCP) server, which can dynamically assign (or “lease”) IP addresses to clients. Selecting Disabled disengages the DHCP server, requiring that you manually assign unique and permanent (or “static”) IP addresses to clients. NOTE: The built-in DHCP Server is a router function. Therefore, this field, and the related DHCP Server fields below, are disabled or ignored if the Operation Mode on the BASIC Page is set to Access Point . NOTE: You will need to disable the DHCP Server , and assign static IP addresses, if you wish to use features on the ROUTING Page. FACTORY DEFAULT: Enabled
DHCP Starting IP Address: (ADVANCED)	Sets the start of the IP address range that the DHCP server will lease to clients. NOTE: This field is ignored if the DHCP Server (above) is Disabled . FACTORY DEFAULT: 192.168.10.2

Field	Description
DHCP Ending IP Address: (ADVANCED)	Sets the end of the IP address range that the DHCP server will lease to clients. By factory default this is set to offer the maximum number of concurrent IP address leases (253). <i>NOTE:</i> This field is ignored if the DHCP Server (above) is Disabled . FACTORY DEFAULT: 192.168.10.254
DHCP Lease Time: (ADVANCED)	Sets the length of time (in seconds) that DHCP leases will be valid. By factory default, this is set at 86,400 seconds, or 24 hours. <i>NOTE:</i> This field is ignored if the DHCP Server (above) is Disabled . FACTORY DEFAULT: 86400
Active DHCP Leases: (DISPLAY ONLY)	Shows a list of the active DHCP leases since the last reboot. For each active lease, the client's host name, MAC address, IP address, and remaining lease duration are shown.

Options related to: OPTIMIZING LOCAL AREA NETWORK ROUTING

Spanning Tree Protocol:

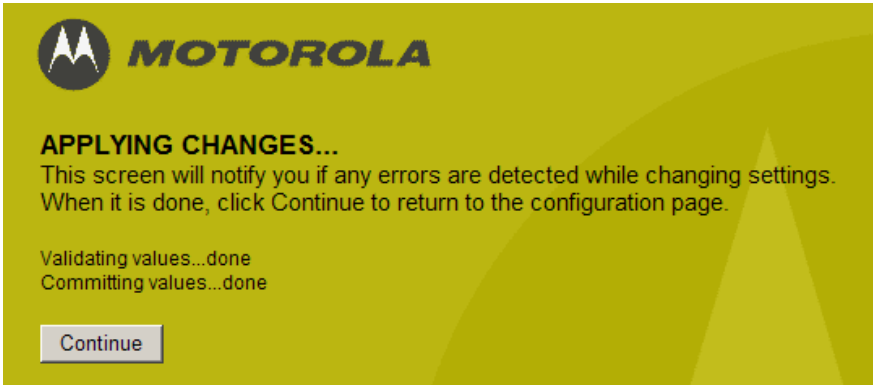
Static Routes:

IP Address	Subnet Mask	Gateway	Metric

Field	Description
Spanning Tree Protocol: (ADVANCED)	Enables use of the Ethernet 802.1d Spanning Tree Protocol, which eliminates bridging loops across the LAN connections. <ul style="list-style-type: none"> Selecting Enabled engages the Spanning Tree Protocol. Selecting Disabled disengages the Spanning Tree Protocol. <i>NOTE:</i> This setting is only used if Operation Mode on the BASIC Page is set to Router . FACTORY DEFAULT: Enabled
Static Routes: (ADVANCED)	Sets static routes to up to five specific clients on your local network. For each route, a Destination IP Address, Subnet Mask, and Gateway must be entered, along with the number of intermediate routers (or "Metric") between this router and the client. <i>NOTE:</i> These settings are only used if Operation Mode on the BASIC Page is set to Router . FACTORY DEFAULT: (blank)

LAN Page Action Buttons

At the bottom of the LAN Page, you will see two clickable buttons to process any desired changes to the configuration options.

Button	Purpose
Apply	<p>This button allows you to apply the settings you have selected for LAN Page configuration options.</p> <p>When you click the Apply button, you will see an “Applying Changes” page that shows the status of validating and committing the new selections that have been made.</p>  <p>If no errors were made in the new selections, the prior selections (including any default settings) will be overridden with your new selections. If errors were made in the new selections, you can return to the LAN Page to correct and re-apply them.</p>
Cancel	<p>Cancels all changes you have made on the LAN Page, reverting the page to its previously saved configuration.</p> <p>Any new selections will be deleted and not be applied.</p>

The WAN (Wide Area Network) Configuration Page

This page allows you to configure your WR850 to support connections to broadband services (via cable, DSL, or other connections to your home or office).

Figure 3-5 Wide Area Network (WAN) Page

MOTOROLA WR850GP

Basic LAN **WAN** Status Filters Routing Wireless Security Firmware

WIDE AREA NETWORK (WAN)
This page allows you to configure your router/access point to support connections to broadband services.

Connection: Default Connection Select
New Delete

Description: Default Connection
Interface: vlan1 (00:0C:E5:51:A6:D1)
Connection Mode: DHCP
Primary: Yes

Host Name:
Domain Name:
MAC Address: 00:0C:E5:51:A6:D1
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Default Gateway: 0.0.0.0
DNS Servers:
WINS Servers:

PPPoE Username:
PPPoE Password:
PPPoE Service Name:
PPPoE Access Concentrator:
PPPoE Connect on Demand: Disabled
PPPoE Max Idle Time: 60
PPPoE Keep Alive: Disabled
PPPoE MRU: 1492
PPPoE MTU: 1492

DDNS Server: Disabled
DDNS User Name:
DDNS User Password:
DDNS Host Name:

Connection Status: Unknown
WAN IP Address Expires In: Expired

Static Routes:	IP Address	Subnet Mask	Gateway	Metric

Apply Cancel Release Renew

WAN Page – Commonly Used Configuration Options

The following configuration options are highlighted in **white** on the WAN Page, for easy reference. These fields are the most commonly used or adjusted, in supporting typical uses of the WR850 as a wired/wireless router.

The rest of the configuration options are provided primarily for advanced users.

Field	Description
Connection Mode:	<p>Sets the method by which an IP address is assigned to the WR850's broadband connection.</p> <p>Select as follows:</p> <p>DHCP - An IP address is dynamically assigned to the WR850, as per the Dynamic Host Configuration Protocol (DHCP). This is typically used with cable modems or gateways, and DSL gateways.</p> <p>Static – An IP address is manually assigned to the WAN connection.</p> <p>PPPoE - Point-to-Point Protocol over Ethernet (PPPoE) is used. PPPoE is typically used with DSL modems.</p> <p>Disabled - The WAN connection is disabled.</p> <p>FACTORY DEFAULT: DHCP</p>
PPPoE Username:	<p>[FOR CONNECTIONS USING PPPoE CONNECTION MODE]</p> <p>Sets the username for authenticating with a Point-to-Point Protocol (PPP) server.</p> <p>This username is provided by your Internet Service Provider (ISP).</p> <p>FACTORY DEFAULT: (blank)</p>
PPPoE Password:	<p>[FOR CONNECTIONS USING PPPoE CONNECTION MODE]</p> <p>Sets the password for authenticating with a PPP server.</p> <p>This password is provided by your ISP.</p> <p>FACTORY DEFAULT: (blank)</p>
PPPoE Service Name:	<p>[FOR CONNECTIONS USING PPPoE CONNECTION MODE]</p> <p>Sets the service name as per information provided by your ISP. May be automatically detected and entered for you; otherwise it will need to be entered manually.</p> <p>FACTORY DEFAULT: (blank)</p>

WAN Page – All Configuration Options

Options related to: SELECTING THE WR850 BROADBAND CONNECTION MODE

The screenshot shows a configuration interface with the following fields and values:

- Connection:** A dropdown menu showing "Default Connection" with a "Select" button next to it.
- New** and **Delete** buttons.
- Description:** A text input field containing "Default Connection".
- Interface:** A dropdown menu showing "vlan1 (00:0C:E5:51:A6:D1)".
- Connection Mode:** A dropdown menu showing "DHCP".
- Primary:** A dropdown menu showing "Yes".

Field	Description
Connection: (ADVANCED)	<p>Your WR850 allows you to store multiple profiles for your broadband connection. This field allows you to select which of multiple connection profiles you wish to configure.</p> <p>Note: You may add additional connections by clicking the New button. You may delete connections by clicking the Delete button.</p> <p>FACTORY DEFAULT: One connection, called "Default Connection."</p>
Description: (ADVANCED)	<p>Sets a name for the selected connection.</p> <p>FACTORY DEFAULT: The first connection is called "Default Connection." New connections default to "Connection [X]", where [X] is a number (e.g., the second connection defaults to "Connection 2").</p>
Interface: (ADVANCED)	<p>Sets the interface used by the selected connection. Currently, the factory default is the only option.</p> <p>FACTORY DEFAULT: The built-in WR850 WAN MAC address.</p>
Connection Mode:	<p>Sets the method by which an IP address is assigned to the selected connection. Select as follows:</p> <p>DHCP - An IP address is dynamically assigned to the WR850, as per the Dynamic Host Configuration Connection Mode (DHCP). This is typically used with cable modems or gateways, and DSL gateways.</p> <p>Static – An IP address is manually assigned to the WAN connection.</p> <p>PPPoE - Point-to-Point Protocol over Ethernet (PPPoE) is used. PPPoE is typically used with DSL modems.</p> <p>Disabled - The WAN connection is disabled.</p> <p>FACTORY DEFAULT: DHCP</p>
Primary: (ADVANCED)	<p>Sets the selected connection to be the primary connection in use. Select Yes or No.</p> <p>FACTORY DEFAULT: Yes</p>

Options related to: SETTING UP A DHCP BROADBAND CONNECTION

Host Name:	<input type="text"/>
Domain Name:	<input type="text"/>
MAC Address:	<input type="text" value="00:0C:E5:51:A6:D1"/>

Field	Description
Host Name: (ADVANCED)	<p>If your Internet Service Provider (ISP) requires a host name when requesting an IP address through DHCP, it can be entered here.</p> <p>FACTORY DEFAULT: (blank)</p>
Domain Name: (ADVANCED)	<p>If your Internet Service Provider (ISP) requires a domain name to be provided when requesting an IP address through DHCP, it can be entered here.</p> <p>FACTORY DEFAULT: (blank)</p>
MAC Address: (ADVANCED)	<p>If your ISP requires that a specific MAC address be used, you can enter that address here.</p> <p>The factory default MAC address is the one built into your WR850, and printed on the product label as "WAN MAC".</p> <p><u>NOTE:</u> A MAC Address has a format of: XX:XX:XX:XX:XX:XX.</p> <p><u>NOTE:</u> WR850 use of an ISP-specific MAC Address is also called "MAC address cloning".</p> <p>FACTORY DEFAULT: The built-in WR850 WAN MAC address</p>

Options related to: SETTING UP A STATIC BROADBAND CONNECTION

IP Address:	<input type="text" value="0.0.0.0"/>
Subnet Mask:	<input type="text" value="0.0.0.0"/>
Default Gateway:	<input type="text" value="0.0.0.0"/>
DNS Servers :	<input type="text"/>
	<input type="text"/>
WINS Servers :	<input type="text"/>
	<input type="text"/>
	<input type="text"/>

Field	Description
IP Address: (ADVANCED)	<p>Sets the IP address of the selected connection.</p> <p>FACTORY DEFAULT: 0.0.0.0</p>

Field	Description
Subnet Mask: (ADVANCED)	Sets the IP Subnet Mask of the selected connection. FACTORY DEFAULT: 0.0.0.0
Default Gateway: (ADVANCED)	Sets the IP address of the default gateway for use on the selected connection. FACTORY DEFAULT: 0.0.0.0
DNS Servers: (ADVANCED)	Sets up to three IP addresses for Domain Name Service (DNS) servers to use for resolving host names. FACTORY DEFAULT: (blank)
WINS Servers: (ADVANCED)	Sets up to three IP addresses for Windows Internet Naming Service (WINS) servers to use for resolving NetBIOS names. FACTORY DEFAULT: (blank)

Options related to: SETTING UP A PPPoE BROADBAND CONNECTION

PPPoE Username:
 PPPoE Password:
 PPPoE Service Name:
 PPPoE Access Concentrator:
 PPPoE Connect on Demand:
 PPPoE Max Idle Time:
 PPPoE Keep Alive:
 PPPoE MRU:
 PPPoE MTU:

Field	Description
PPPoE Username:	Sets the username for authenticating with a Point-to-Point Protocol (PPP) server. This username is provided by your ISP. FACTORY DEFAULT: (blank)
PPPoE Password:	Sets the password for authenticating with a PPP server. This password is provided by your ISP. FACTORY DEFAULT: (blank)
PPPoE Service Name:	Sets the service name as per information provided by your ISP. May be automatically detected and entered for you; otherwise it will need to be entered manually. FACTORY DEFAULT: (blank)

Field	Description
PPPoE Access Concentrator: (ADVANCED)	Sets the name of the PPP access concentrator, as may be required by some ISPs. FACTORY DEFAULT: (blank)
PPPoE Connect on Demand: (ADVANCED)	Sets whether the PPP connection should be automatically disconnected if no traffic has been observed for the period specified by <i>PPPoE Max Idle Time</i> . <ul style="list-style-type: none"> Selecting Enabled engages this automatic disconnection. Selecting Disabled suppresses automatic disconnection. FACTORY DEFAULT: Disabled
PPPoE Max Idle Time: (ADVANCED)	Sets the number of seconds to wait before disconnecting the PPPoE connection if <i>PPPoE Connect on Demand</i> is Enabled. This value can be anywhere between 1 and 3600 seconds. FACTORY DEFAULT: 60
PPPoE Keep Alive: (ADVANCED)	Sets whether or not the PPPoE connection should be automatically restored if it is lost. <ul style="list-style-type: none"> Selecting Enabled automatically restores lost connections. Selecting Disabled suppresses automatic re-connection. <p><i>NOTE:</i> <i>This setting has no effect unless PPPoE Connect on Demand (above) is Disabled.</i></p> FACTORY DEFAULT: Disabled
PPPoE MRU: (ADVANCED)	Sets the maximum number of bytes that the PPPoE connection will <u>receive</u> in a single Ethernet frame. This value can be anywhere between 128 and 9999 bytes. FACTORY DEFAULT: 1492
PPPoE MTU: (ADVANCED)	Sets the maximum number of bytes that the PPPoE connection will <u>transmit</u> in a single Ethernet frame. This value can be anywhere between 128 and 9999 bytes. FACTORY DEFAULT: 1492

Options related to: SETTING UP A LINK TO A DYNAMIC DOMAIN NAME SERVICE

DDNS Server:	Disabled <input type="button" value="v"/>
DDNS User Name:	<input type="text"/>
DDNS User Password:	<input type="text"/>
DDNS Host Name:	<input type="text"/>

Field	Description
DDNS Server: (ADVANCED)	<p>The WR850 supports a feature called Dynamic Domain Name System (DDNS), which enables you to assign a fixed host and domain name to a dynamic Internet IP address (e.g., an IP address assigned to the WR850 through DHCP).</p> <p>DDNS is particularly useful if you are hosting your own web server, FTP server, or other type of server behind the router, so that visitors can locate your service with a consistent name.</p> <p>Before you can use this feature, you must sign up for DDNS service at a DDNS service provider, such as www.dyndns.org or www.changeip.com.</p> <p>Once you have signed up, you can enable the feature by selecting the appropriate DDNS service provider.</p> <p>FACTORY DEFAULT: Disabled</p>
User Name: (ADVANCED)	<p>The DDNS service provider will assign you a User Name when you sign up for service.</p> <p>That User Name should be entered in this field.</p> <p><u>NOTE:</u> DDNS Server (above) must be enabled with a service provider in order to modify this field.</p> <p>FACTORY DEFAULT: (blank)</p>
User Password: (ADVANCED)	<p>The DDNS service provider will assign you a User Password when you sign up for service.</p> <p>That User Password should be entered in this field.</p> <p><u>NOTE:</u> DDNS Server (above) must be enabled with a service provider in order to modify this field.</p> <p>FACTORY DEFAULT: (blank)</p>
Host Name: (ADVANCED)	<p>Sets the fully qualified domain name registered for your WAN connection.</p> <p><u>NOTE:</u> DDNS Server (above) must be enabled with a service provider in order to modify this field.</p> <p>FACTORY DEFAULT: (blank)</p>

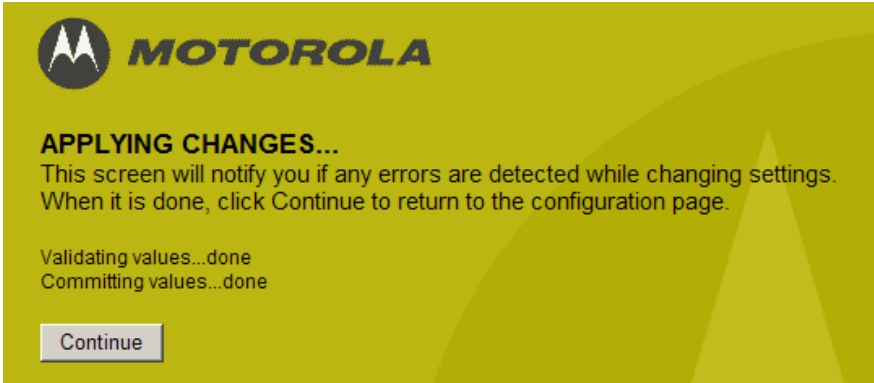
Options related to: OPTIMIZING WAN ROUTING

Connection Status: Unknown				
WAN IP Address Expires In: Expired				
Static Routes:	IP Address	Subnet Mask	Gateway	Metric

Field	Description
Connection Status: (DISPLAY ONLY)	Shows the state of the selected connection.
IP Address Expires In: (DISPLAY ONLY)	Shows the time left on the current IP address leased to the WR850. Shows Expired when address has elapsed.
Static Routes: (ADVANCED)	Sets static routes to up to five specific clients over the broadband connection. For each route, a Destination IP Address, Subnet Mask, and Gateway must be entered, along with the number of intermediate routers (or "Metric") between this router and the client. <i>NOTE:</i> These settings are only used if Operation Mode on the BASIC Page is set to Router . FACTORY DEFAULT: (blank)

WAN Page Action Buttons

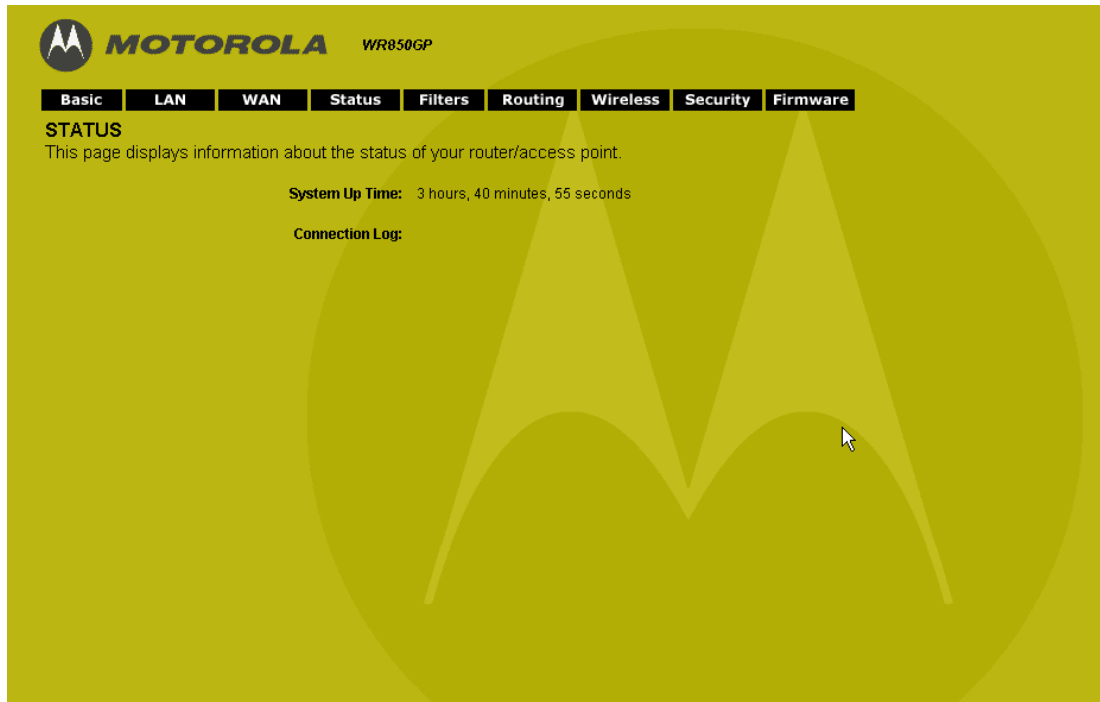
At the bottom of the WAN Page, you will see four clickable buttons to process any desired changes to the configuration options.

Button	Purpose
Apply	<p>This button allows you to apply the settings you have selected for WAN Page configuration options.</p> <p>When you click the Apply button, you will see an “Applying Changes” page that shows the status of validating and committing the new selections that have been made.</p>  <p>If no errors were made in the new selections, the prior selections (including any default settings) will be overridden with your new selections. If errors were made in the new selections, you can return to the WAN Page to correct and re-apply them.</p>
Cancel	<p>Cancels all changes you have made on the WAN Page, reverting the page to its previously saved configuration.</p> <p>Any new selections will be deleted and not be applied.</p>
Release	<p>Releases the current IP address leased to the selected WR850 WAN connection.</p>
Renew	<p>Renews the IP address lease for the selected WR850 WAN connection.</p>

The STATUS Configuration Page

This page allows you to view key reporting information about your WR850.

Figure 3-6 STATUS Page



STATUS Page Configuration Options

Field	Description
System Up Time: (DISPLAY ONLY)	Shows the length of time for which the WR850 has been operating since it was last booted. Shows the time in hours, minutes and seconds [e.g., 2 hours, 4 minutes, 30 seconds].
Connection Log: (DISPLAY ONLY)	Shows a log of recent client connections to the WR850, as per the <i>Connection Logging</i> selection made on the BASIC Page. Connections are typically listed with: <ul style="list-style-type: none">• the date and time the connection was made,• the communication Connection Mode used,• the IP address of the connecting client, and• the ports used on the WR850 for the connected client.

The FILTERS Configuration Page

This page allows you to configure two types of filters, allowing you to block undesired use of your broadband connection.

One potential use of these filters is to set parental controls on the use of the Internet.

Figure 3-6 FILTERS Page

MOTOROLA WR850GP

Basic LAN WAN Status **FILTERS** Routing Wireless Security Firmware

FILTERS
This page allows you to configure two types of filters, allowing you to block undesired use of your broadband connection. One potential use of these filters is to set parental controls on the use of the Internet.

LAN MAC Filter Mode: Deny

Filtered LAN MAC Addresses:

LAN IP Address Range	Protocol	Destination Port Range	From Day	To Day	From Hour	To Hour	Enabled
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>

Apply Cancel

FILTERS Page – Commonly Used Configuration Options

None of the configuration options on the FILTERS Page typically require any adjustment from factory defaults to support most typical uses of the WR850 as a wired/wireless router.

Therefore, none of the configuration options on the FILTERS Page are highlighted in **white**. FILTERS Page configuration options are provided primarily for advanced users.

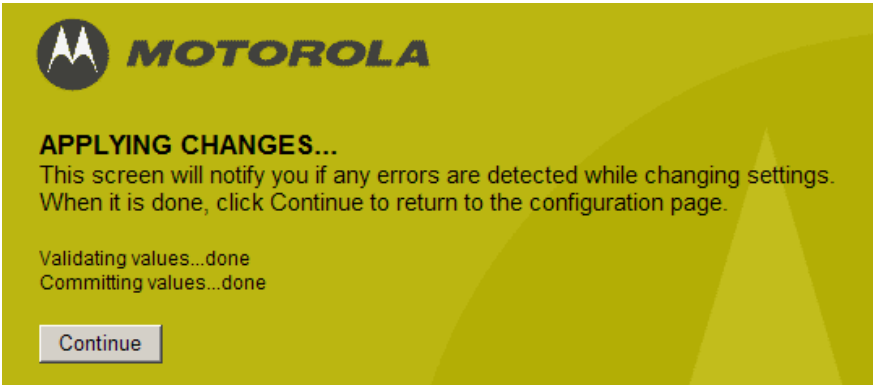
FILTERS Page – All Configuration Options

Field	Description
LAN MAC Filter Mode: (ADVANCED)	<p>Sets whether local network clients (specified by MAC address) are allowed or denied access to your broadband connection.</p> <ul style="list-style-type: none"> • Selecting Allow will allow access only by the clients identified by the <i>Filtered LAN MAC Addresses</i> below. • Selecting Deny will deny access by the clients identified by the <i>Filtered LAN MAC Addresses</i> below. • Selecting Disabled will suppress all MAC address filtering, and allow all clients access to your broadband connection. <p>FACTORY DEFAULT: Deny</p>
Filtered LAN MAC Addresses: (ADVANCED)	<p>Sets a list of up to 10 LAN clients (specified by MAC address) from which communications are filtered as per the <i>LAN MAC Filter Mode</i>.</p> <p>NOTE: A MAC address has a format of: XX:XX:XX:XX:XX:XX.</p> <p>FACTORY DEFAULT: (blank)</p>
LAN Usage Filters: (ADVANCED)	<p>Sets rules whereby LAN clients (specified by IP address) are not allowed access to certain port ranges during specified times. For example, clients might be temporarily blocked from Internet use.</p> <p>NOTE: These settings are only used if Operation Mode on the <i>BASIC Page</i> is set to Router.</p> <p>You can store up to 20 filtering rules, and selectively enable one or more of them when desired, using the Enabled checkbox at the end of each row.</p> <p>NOTE: Filtering rules will be applied in the order in which they are listed on this page.</p> <p>For each filtering rule, the following 5 items must be entered:</p> <p>(1) LAN IP Address Range:</p> <p>These two fields define a range of LAN clients to which the filtering rule will apply. To apply a rule to a specific client, enter the same IP address in both fields.</p> <p>FACTORY DEFAULT: (blank)</p> <p>(2) Protocol:</p> <p>This field specifies the Internet communication Protocol that will be restricted as per the filtering rule.</p> <p style="text-align: right;"><i>(continued on next page)</i></p>

Field	Description
LAN Usage Filters: (continued)	<ul style="list-style-type: none"> Selecting TCP restricts use of the Transmission Control Protocol, an end-to-end protocol defining rules and procedures for data exchange between hosts. Selecting UDP restricts use of the User Datagram Protocol, which is used in conjunction with the Internet Protocol (IP) to send data in the form of message units. <p>FACTORY DEFAULT: TCP</p> <p>(3) Destination Port Range:</p> <p>These two fields define a range of ports to which the filtering rule will apply. To apply a rule to a specific port, enter the same port number in both fields.</p> <p>FACTORY DEFAULT: (blank)</p> <p>(4) Days-of-the-Week Range:</p> <p>These two fields define a range of days of the week on which the filtering rule will apply. The From Day will be the first day of the week on which the rule will apply; the To Day will be the first day of the week on which the rule will not apply.</p> <p>To apply a rule continuously, select the same From Day and To Day.</p> <p>FACTORY DEFAULT: From Sunday To Sunday (continuous)</p> <p>(5) Hours-of-the-Day Range:</p> <p>These two fields define a range of hours of the day on which the filtering rule will apply. This range will apply equally to all days selected in the Days-of-the-Week Range.</p> <p>The From Hour will be the first hour of the day during which the rule will apply. The rule will be applied until the beginning of the To Hour.</p> <p>To apply a rule continuously, select 12:00AM for both From Hour and To Hour.</p> <p>FACTORY DEFAULT: From 12:00AM To 12:00AM (continuous)</p>

FILTERS Page Action Buttons

At the bottom of the FILTERS Page, you will see two click-able buttons to process any desired changes to the configuration options.

Button	Purpose
Apply	<p>This button allows you to apply the settings you have selected for FILTERS Page configuration options.</p> <p>When you click the Apply button, you will see an “Applying Changes” page that shows the status of validating and committing the new selections that have been made.</p>  <p>If no errors were made in the new selections, the prior selections (including any default settings) will be overridden with your new selections. If errors were made in the new selections, you can return to the FILTERS Page to correct and re-apply them.</p>
Cancel	<p>Cancels all changes you have made on the FILTERS Page, reverting the page to its previously saved configuration.</p> <p>Any new selections will be deleted and not be applied.</p>

FILTERS Page Examples – Establishing Parental Controls on Internet Use

The WR850 filters can allow you to restrict use of your broadband connection in a variety of ways:

- Blocking use of the Internet at one or more PCs in your home, at all times
(e.g., *there is a dedicated PC in the home for homework, where Internet surfing is not required*)
- Blocking use of the Internet at one or more PCs in your home, at particular times
(e.g., *when homework is to be done, and does not require Internet surfing*)
- Blocking specific uses of the Internet at one or more PCs in your home, at particular times
(e.g., *when homework is to be done, and neither Internet gaming nor Internet messaging should be in use*).

The following examples demonstrate these three types of parental controls on your WR850.

Blocking Internet Use at All Times – Using MAC Addresses

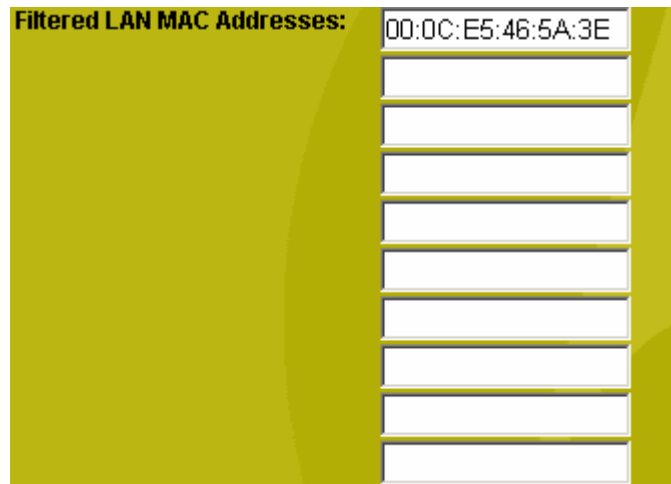
For this example, we assume that:

- there is one PC to be restricted, and
- the MAC address of that PC is 00:0C:E5:51:A6:D1.

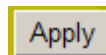
Step 1: At the *LAN MAC Filter Mode*, select **Deny**.

A screenshot of a web interface showing a dropdown menu. The text "LAN MAC Filter Mode:" is followed by a dropdown box that currently displays "Deny".

Step 2: At *Filtered LAN MAC Addresses*, enter the MAC address(es) of the PC(s) to be restricted.

A screenshot of a web interface showing a section titled "Filtered LAN MAC Addresses:". To the right of the title is a text input field containing the MAC address "00:0C:E5:46:5A:3E". Below this input field are eight more empty text input fields, all contained within a yellow-shaded rectangular area.

Step 3: At the bottom of the page, click the *Apply* action button.

A screenshot of a button labeled "Apply". The button has a yellow border and a light blue background.

Blocking Internet Use at All Times – Using IP Addresses

For this example, we assume that:

- there is one PC to be restricted, and
- the IP address assigned to that PC is 192.168.10.4.

Step 1: At *LAN Usage Filters*, under *LAN IP Address Range*, on consecutive lines enter the IP address(es) of the PC(s) to be restricted.

LAN Usage Filters:		LAN IP Address Range	Protocol	Destination Port Range	From Day	To Day	From Hour	To Hour	Enabled
		192.168.10.4 - 192.168.10.4	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
		192.168.10.4 - 192.168.10.4	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>

NOTE: If you intend to restrict multiple clients in the home, it is best to assign them consecutive IP addresses, to allow you to enter a single LAN IP Address Range without disabling another client.

Step 2: Under *Protocol*, select **TCP** on one line and **UDP** on the next.

LAN Usage Filters:		LAN IP Address Range	Protocol	Destination Port Range	From Day	To Day	From Hour	To Hour	Enabled
		192.168.10.4 - 192.168.10.4	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
		192.168.10.4 - 192.168.10.4	UDP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>

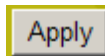
Step 3: Under *Destination Port Range*, enter the entire port range (0 through 65535) on both lines.

LAN Usage Filters:		LAN IP Address Range	Protocol	Destination Port Range	From Day	To Day	From Hour	To Hour	Enabled
		192.168.10.4 - 192.168.10.4	TCP	0 - 65535	Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
		192.168.10.4 - 192.168.10.4	UDP	0 - 65535	Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>

Step 4: At the end of each line, check the *Enabled* box to engage the filters.

LAN Usage Filters:		LAN IP Address Range	Protocol	Destination Port Range	From Day	To Day	From Hour	To Hour	Enabled
		192.168.10.4 - 192.168.10.4	TCP	0 - 65535	Sunday	Sunday	12:00 AM	12:00 AM	<input checked="" type="checkbox"/>
		192.168.10.4 - 192.168.10.4	UDP	0 - 65535	Sunday	Sunday	12:00 AM	12:00 AM	<input checked="" type="checkbox"/>

Step 5: At the bottom of the page, click the *Apply* action button.



Blocking Internet Use at Particular Times

When using the *LAN Usage Filters*, you have the additional opportunity to establish Internet controls that run between particular times. There are two ways to do this:

- (1) The “manual” approach: Enter the Web-based Configuration Utility at the beginning and end of restriction periods to enable and disable continuous filters by checking and un-checking the *Enabled* boxes at the end of each line.
- (2) The “automated” approach: Use day and time settings on *LAN Usage Filters*, automatically engaging and suppressing the restrictions at desired times.

For this example, we assume that:

- the “automated” approach is desired,
- there is one PC to be restricted,
- the IP address assigned to that PC is 192.168.10.4, and
- the PC is to be restricted from 6 PM to 8 PM, Monday through Friday.

Step 1: At *LAN Usage Filters*, under *LAN IP Address Range*, enter the IP address(es) of the PC(s) to be restricted.

LAN Usage Filters:	LAN IP Address Range		Protocol	Destination Port Range		From Day	To Day	From Hour	To Hour	Enabled
	192.168.10.4	192.168.10.4	TCP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	192.168.10.4	192.168.10.4	TCP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	192.168.10.4	192.168.10.4	TCP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	192.168.10.4	192.168.10.4	TCP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	192.168.10.4	192.168.10.4	TCP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	192.168.10.4	192.168.10.4	TCP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	192.168.10.4	192.168.10.4	TCP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	192.168.10.4	192.168.10.4	TCP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	192.168.10.4	192.168.10.4	TCP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	192.168.10.4	192.168.10.4	TCP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>

NOTE: If you intend to restrict multiple clients in the home, it is best to assign them consecutive IP addresses to allow you to enter a single LAN IP Address Range without disabling another client, while conserving LAN Usage Filters at the same time.

Step 2: Under *Protocol*, alternate **TCP** and **UDP** on each line.

LAN Usage Filters:	LAN IP Address Range		Protocol	Destination Port Range		From Day	To Day	From Hour	To Hour	Enabled
	192.168.10.4	192.168.10.4	TCP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	192.168.10.4	192.168.10.4	UDP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	192.168.10.4	192.168.10.4	TCP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	192.168.10.4	192.168.10.4	UDP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	192.168.10.4	192.168.10.4	TCP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	192.168.10.4	192.168.10.4	UDP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	192.168.10.4	192.168.10.4	TCP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	192.168.10.4	192.168.10.4	UDP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	192.168.10.4	192.168.10.4	TCP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>
	192.168.10.4	192.168.10.4	UDP			Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>

Step 3: Under *Destination Port Range*, enter the entire port range (0 through 65535) on each line.

LAN Usage Filters:		LAN IP Address Range		Protocol	Destination Port Range		From Day	To Day	From Hour	To Hour	Enabled
		192.168.10.4	192.168.10.4	TCP ▾	0	65535	Sunday ▾	Sunday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	UDP ▾	0	65535	Sunday ▾	Sunday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	TCP ▾	0	65535	Sunday ▾	Sunday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	UDP ▾	0	65535	Sunday ▾	Sunday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	TCP ▾	0	65535	Sunday ▾	Sunday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	UDP ▾	0	65535	Sunday ▾	Sunday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	TCP ▾	0	65535	Sunday ▾	Sunday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	UDP ▾	0	65535	Sunday ▾	Sunday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	TCP ▾	0	65535	Sunday ▾	Sunday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	UDP ▾	0	65535	Sunday ▾	Sunday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>

Step 4: Under *From Day* and *To Day*, select the first day the restrictions should be in place, and then the first day the restrictions should no longer be in place.

If a filtering period begins and ends on the same day, the same day should be entered in *From Day* and *To Day*. If that same filtering period is repeated on multiple days, you should enter each day on a pair of filter lines:

LAN Usage Filters:		LAN IP Address Range		Protocol	Destination Port Range		From Day	To Day	From Hour	To Hour	Enabled
		192.168.10.4	192.168.10.4	TCP ▾	0	65535	Monday ▾	Monday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	UDP ▾	0	65535	Monday ▾	Monday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	TCP ▾	0	65535	Tuesday ▾	Tuesday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	UDP ▾	0	65535	Tuesday ▾	Tuesday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	TCP ▾	0	65535	Wednesday ▾	Wednesday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	UDP ▾	0	65535	Wednesday ▾	Wednesday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	TCP ▾	0	65535	Thursday ▾	Thursday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	UDP ▾	0	65535	Thursday ▾	Thursday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	TCP ▾	0	65535	Friday ▾	Friday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	UDP ▾	0	65535	Friday ▾	Friday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>

Step 5: Under *From Hour* and *To Hour*, select the start and stop times of the restrictions that will be in place.

LAN Usage Filters:		LAN IP Address Range		Protocol	Destination Port Range		From Day	To Day	From Hour	To Hour	Enabled
		192.168.10.4	192.168.10.4	TCP ▾	0	65535	Monday ▾	Monday ▾	6:00 PM ▾	8:00 PM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	UDP ▾	0	65535	Monday ▾	Monday ▾	6:00 PM ▾	8:00 PM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	TCP ▾	0	65535	Tuesday ▾	Tuesday ▾	6:00 PM ▾	8:00 PM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	UDP ▾	0	65535	Tuesday ▾	Tuesday ▾	6:00 PM ▾	8:00 PM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	TCP ▾	0	65535	Wednesday ▾	Wednesday ▾	6:00 PM ▾	8:00 PM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	UDP ▾	0	65535	Wednesday ▾	Wednesday ▾	6:00 PM ▾	8:00 PM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	TCP ▾	0	65535	Thursday ▾	Thursday ▾	6:00 PM ▾	8:00 PM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	UDP ▾	0	65535	Thursday ▾	Thursday ▾	6:00 PM ▾	8:00 PM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	TCP ▾	0	65535	Friday ▾	Friday ▾	6:00 PM ▾	8:00 PM ▾	<input type="checkbox"/>
		192.168.10.4	192.168.10.4	UDP ▾	0	65535	Friday ▾	Friday ▾	6:00 PM ▾	8:00 PM ▾	<input type="checkbox"/>

Step 6: At the end of each line, check the *Enabled* box to engage the filters.

LAN Usage Filters:	LAN IP Address Range		Protocol	Destination Port Range		From Day	To Day	From Hour	To Hour	Enabled
	192.168.10.4	192.168.10.4	TCP	0	65535	Monday	Monday	6:00 PM	8:00 PM	<input checked="" type="checkbox"/>
	192.168.10.4	192.168.10.4	UDP	0	65535	Monday	Monday	6:00 PM	8:00 PM	<input checked="" type="checkbox"/>
	192.168.10.4	192.168.10.4	TCP	0	65535	Tuesday	Tuesday	6:00 PM	8:00 PM	<input checked="" type="checkbox"/>
	192.168.10.4	192.168.10.4	UDP	0	65535	Tuesday	Tuesday	6:00 PM	8:00 PM	<input checked="" type="checkbox"/>
	192.168.10.4	192.168.10.4	TCP	0	65535	Wednesday	Wednesday	6:00 PM	8:00 PM	<input checked="" type="checkbox"/>
	192.168.10.4	192.168.10.4	UDP	0	65535	Wednesday	Wednesday	6:00 PM	8:00 PM	<input checked="" type="checkbox"/>
	192.168.10.4	192.168.10.4	TCP	0	65535	Thursday	Thursday	6:00 PM	8:00 PM	<input checked="" type="checkbox"/>
	192.168.10.4	192.168.10.4	UDP	0	65535	Thursday	Thursday	6:00 PM	8:00 PM	<input checked="" type="checkbox"/>
	192.168.10.4	192.168.10.4	TCP	0	65535	Friday	Friday	6:00 PM	8:00 PM	<input checked="" type="checkbox"/>
192.168.10.4	192.168.10.4	UDP	0	65535	Friday	Friday	6:00 PM	8:00 PM	<input checked="" type="checkbox"/>	

Step 7: At the bottom of the page, click the *Apply* action button.

Apply

Blocking Specific Types of Internet Use at Particular Times

When using the *LAN Usage Filters*, you have the additional opportunity to establish Internet controls on specific ports. Since some Internet applications will open and close specific ports in order to function, you can block the use of those applications by specific client PCs by blocking the use of those ports by those PCs.

For this example, we assume that:

- there is one PC to be restricted,
- the IP address assigned to that PC is 192.168.10.4,
- the PC is to be restricted from using an Internet game Monday through Friday, all day, and
- the Internet game to be restricted requires port 28910 for TCP communications.

Step 1: At *LAN Usage Filters*, under *LAN IP Address Range*, enter the IP address(es) of the PC(s) to be restricted.

LAN Usage Filters:	LAN IP Address Range		Protocol	Destination Port Range		From Day	To Day	From Hour	To Hour	Enabled
	192.168.10.4	192.168.10.4	TCP ▾			Sunday ▾	Sunday ▾	12:00 AM ▾	12:00 AM ▾	<input type="checkbox"/>

NOTE: If you intend to restrict multiple clients in the home, it is best to assign them consecutive IP addresses, to allow you to enter a single LAN IP Address Range without disabling another client, while conserving LAN Usage Filters at the same time.

Step 2: Under *Protocol*, select the protocol which applies to the communications to be restricted.

LAN Usage Filters:	LAN IP Address Range	Protocol	Destination Port Range	From Day	To Day	From Hour	To Hour	Enabled
	192.168.10.4 - 192.168.10.4	TCP		Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>

Step 3: Under *Destination Port Range*, enter the port(s) to be restricted.

LAN Usage Filters:	LAN IP Address Range	Protocol	Destination Port Range	From Day	To Day	From Hour	To Hour	Enabled
	192.168.10.4 - 192.168.10.4	TCP	28910 - 28910	Sunday	Sunday	12:00 AM	12:00 AM	<input type="checkbox"/>

Step 4: Under *From Day* and *To Day*, select the first day the restrictions should be in place, and then the first day the restrictions should no longer be in place.

LAN Usage Filters:	LAN IP Address Range	Protocol	Destination Port Range	From Day	To Day	From Hour	To Hour	Enabled
	192.168.10.4 - 192.168.10.4	TCP	28910 - 28910	Monday	Saturday	12:00 AM	12:00 AM	<input type="checkbox"/>

Step 5: Under *From Hour* and *To Hour*, select the start and stop times of the restrictions that will be in place.

LAN Usage Filters:	LAN IP Address Range	Protocol	Destination Port Range	From Day	To Day	From Hour	To Hour	Enabled
	192.168.10.4 - 192.168.10.4	TCP	28910 - 28910	Monday	Saturday	12:00 AM	12:00 AM	<input type="checkbox"/>

Step 6: At the end of each line, check the *Enabled* box to engage the filters.

LAN Usage Filters:	LAN IP Address Range	Protocol	Destination Port Range	From Day	To Day	From Hour	To Hour	Enabled
	192.168.10.4 - 192.168.10.4	TCP	28910 - 28910	Monday	Saturday	12:00 AM	12:00 AM	<input checked="" type="checkbox"/>

Step 7: At the bottom of the page, click the *Apply* action button.

Apply

The ROUTING Configuration Page

This page allows you to configure port forwarding and triggering rules for your WR850. These rules can allow specific clients on your local network to run and share certain programs that use the Internet.

Figure 3-5 ROUTING Page

MOTOROLA WR850GP

Basic LAN WAN Status Filters **ROUTING** Wireless Security Firmware

ROUTING
This page allows you to configure port forwarding and triggering rules, as needed to allow specific clients on your local network to run and share certain programs that use the Internet.

DMZ IP Address:

Port Forwards:

Protocol	WAN Port Start	WAN Port End	LAN IP Address	LAN Port Start	LAN Port End	Enabled
TCP						<input type="checkbox"/>
TCP						<input type="checkbox"/>
TCP						<input type="checkbox"/>
TCP						<input type="checkbox"/>
TCP						<input type="checkbox"/>
TCP						<input type="checkbox"/>
TCP						<input type="checkbox"/>
TCP						<input type="checkbox"/>
TCP						<input type="checkbox"/>
TCP						<input type="checkbox"/>
TCP						<input type="checkbox"/>
TCP						<input type="checkbox"/>
TCP						<input type="checkbox"/>
TCP						<input type="checkbox"/>
TCP						<input type="checkbox"/>
TCP						<input type="checkbox"/>
TCP						<input type="checkbox"/>
TCP						<input type="checkbox"/>
TCP						<input type="checkbox"/>

Port Triggers:

Outbound Protocol	Outbound Port Start	Outbound Port End	Inbound Protocol	Inbound Port Start	Inbound Port End	To Port Start	To Port End	Enabled
TCP			TCP					<input type="checkbox"/>
TCP			TCP					<input type="checkbox"/>
TCP			TCP					<input type="checkbox"/>
TCP			TCP					<input type="checkbox"/>
TCP			TCP					<input type="checkbox"/>
TCP			TCP					<input type="checkbox"/>
TCP			TCP					<input type="checkbox"/>
TCP			TCP					<input type="checkbox"/>
TCP			TCP					<input type="checkbox"/>
TCP			TCP					<input type="checkbox"/>
TCP			TCP					<input type="checkbox"/>
TCP			TCP					<input type="checkbox"/>
TCP			TCP					<input type="checkbox"/>
TCP			TCP					<input type="checkbox"/>
TCP			TCP					<input type="checkbox"/>
TCP			TCP					<input type="checkbox"/>
TCP			TCP					<input type="checkbox"/>
TCP			TCP					<input type="checkbox"/>
TCP			TCP					<input type="checkbox"/>

Apply Cancel

ROUTING Page – Commonly Used Configuration Options

None of the configuration options on the ROUTING Page typically require any adjustment from factory defaults, to support most typical uses of the WR850 as a wired/wireless router.

Therefore, none of the configuration options on the ROUTING Page are highlighted in **white**. ROUTING Page configuration options are provided primarily for advanced users.

ROUTING Page – All Configuration Options

Field	Description
DMZ IP Address: (ADVANCED)	<p>Sets one device on your local network (specified by IP address) to be a De-militarized Zone (DMZ).</p> <p>A DMZ receives all broadband communication requests that might otherwise be blocked by the router's firewall, as is often needed for real-time Internet gaming.</p> <p>Leave this field blank if no DMZ is desired.</p> <p><u>NOTE:</u> This setting is only used if Operation Mode on the BASIC Page is set to Router.</p> <p>FACTORY DEFAULT: (blank)</p>
Port Forwards: (ADVANCED)	<p>Sets rules for forwarding inbound broadband communications, destined to specific WAN ports, to specific clients on your local network (specified by IP address). You may optionally specify a destination port range, on the LAN side of the WR850, as well.</p> <p>This feature can be particularly useful to support a web server, or other special service, on your local network.</p> <p><u>NOTE:</u> These settings are only used if Operation Mode on the BASIC Page is set to Router.</p> <p>You can store up to 20 port forwarding rules, and selectively enable one or more of them when desired, using the Enabled checkbox at the end of each row.</p> <p><u>NOTE:</u> Port forwards will be applied in the order in which they are listed on this page.</p> <p>For each port forward, the following 3 items can be entered:</p> <p>(1) WAN Port Range:</p> <p>These two fields ("Start" and "End") define a range of WAN ports that will be monitored as part of the port forward. <i>(continued on next page)</i></p>

Port Forwards: (continued)	<p>To forward communications from a single port, enter the same port number in both fields.</p> <p>This information must be entered for each port forward.</p> <p>FACTORY DEFAULT: (blank)</p> <p>(2) LAN IP Address:</p> <p>Sets the client on your local network (specified by IP address) to which communications will be forwarded.</p> <p>This information must be entered for each port forward.</p> <p>FACTORY DEFAULT: (blank)</p> <p>(3) LAN Port Range:</p> <p>These two fields (“Start” and “End”) define a range of LAN ports to which communications will be forwarded. To forward to a single port, enter the same port number in both fields.</p> <p>This information is optional for each port forward.</p> <p>FACTORY DEFAULT: (blank)</p>
Port Triggers: (ADVANCED)	<p>Sets rules for forwarding inbound communications (from your broadband connection) based on specific outbound communications (or “triggers”) from a LAN client.</p> <p>Specifically, if a LAN client transmits to the Internet using any of a set of outbound destination ports, they will be forwarded Internet responses that are received on a corresponding set of inbound destination ports.</p> <p>You may optionally specify a destination port range for forwards, on the LAN side of the WR850, as well.</p> <p>This feature can be particularly useful to support real-time games which require Internet responses to game activity. These responses might otherwise be blocked by the WR850 firewall.</p> <p><u>NOTE:</u> These settings are only used if Operation Mode on the BASIC Page is set to Router.</p> <p>You can store up to 20 port triggers, and selectively enable one or more of them when desired, using the Enabled checkbox at the end of each row. If more port triggers are required, especially for a single client, you should consider configuring the client as a DMZ.</p> <p><u>NOTE:</u> Port triggers will be applied in the order in which they are listed on this page.</p> <p style="text-align: right;">(continued on next page)</p>

Port Triggers: <i>(continued)</i>	<p>For each port trigger, the following 5 items can be entered:</p> <p>(1) Outbound Protocol:</p> <p>This field specifies the Internet communication protocol that will be monitored on specified outbound ports.</p> <ul style="list-style-type: none"> • Selecting TCP monitors the Transmission Control Protocol, an end-to-end protocol defining rules and procedures for data exchange between hosts. • Selecting UDP monitors the User Datagram Protocol, which is used in conjunction with the Internet Protocol (IP) to send data in the form of message units. <p>This selection must be made for each port trigger.</p> <p>FACTORY DEFAULT: TCP</p> <p>(2) Outbound Port Range:</p> <p>These two fields ("Start" and "End") define a range of outbound destination ports that will be monitored as part of the port trigger. To monitor a single port, enter the same port number in both fields.</p> <p>This information must be entered for each port trigger.</p> <p>FACTORY DEFAULT: (blank)</p> <p>(3) Inbound Protocol:</p> <p>This field specifies the Internet communication protocol that will be monitored, for forwarding in response to the outbound trigger.</p> <p>Selections are TCP and UDP, as was the case when selecting the Outbound Protocol.</p> <p>This selection must be made for each port trigger.</p> <p>FACTORY DEFAULT: TCP</p> <p>(4) Inbound Port Range:</p> <p>These two fields ("Start" and "End") define a range of inbound destination ports on the WAN connection that will be monitored in response to the port trigger. To monitor communications from a single port, enter the same port number in both fields.</p> <p>This information must be entered for each port trigger.</p> <p>FACTORY DEFAULT: (blank)</p> <p>(5) To Port Range:</p> <p>These two fields ("Start" and "End") define a range of LAN ports to which communications will be forwarded, in response to the port</p> <p style="text-align: right;"><i>(continued on next page))</i></p>
---	--

Port Triggers:
(continued)

trigger. To forward communications to a single port, enter the same port number in both fields.

This information is optional for each port trigger.

FACTORY DEFAULT: (blank)

Below are common Port Trigger entries for some popular Internet applications:

AOL® Instant Messenger™

- (1) Outbound Protocol: TCP
- (2) Outbound Port Range: 5190
- (3) Inbound Protocol: TCP
- (4) Inbound Port Range: 5190

DirectX® 7

- (1) Outbound Protocol: TCP
 - (2) Outbound Port Range: 47624
 - (3) Inbound Protocol: TCP
 - (4) Inbound Port Range: 2300-2400
- and

- (1) Outbound Protocol: TCP
- (2) Outbound Port Range: 47624
- (3) Inbound Protocol: UDP
- (4) Inbound Port Range: 2300-2400

DirectX® 8

- (1) Outbound Protocol: UDP
- (2) Outbound Port Range: 6073
- (3) Inbound Protocol: UDP
- (4) Inbound Port Range: 2302-2400

Net2Phone®

- (1) Outbound Protocol: UDP
- (2) Outbound Port Range: 6801
- (3) Inbound Protocol: UDP
- (4) Inbound Port Range: 6801

NetMeeting® and H.323

- (1) Outbound Protocol: TCP
- (2) Outbound Port Range: 1720
- (3) Inbound Protocol: TCP
- (4) Inbound Port Range: 1024-65534

and

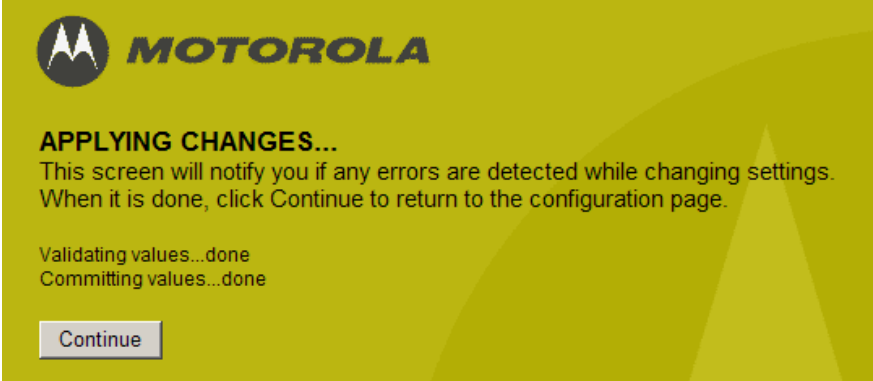
- (1) Outbound Protocol: TCP
- (2) Outbound Port Range: 1720
- (3) Inbound Protocol: UDP
- (4) Inbound Port Range: 1024-65534

QuickTime®

- (1) Outbound Protocol: TCP
- (2) Outbound Port Range: 554
- (3) Inbound Protocol: UDP
- (4) Inbound Port Range: 6970-6999

ROUTING Page Action Buttons

At the bottom of the ROUTING Page, you will see two clickable buttons to process any desired changes to the configuration options.

Button	Purpose
Apply	<p>This button allows you to apply the settings you have selected for ROUTING Page configuration options.</p> <p>When you click the Apply button, you will see an “Applying Changes” page that shows the status of validating and committing the new selections that have been made.</p>  <p>If no errors were made in the new selections, the prior selections (including any default settings) will be overridden with your new selections. If errors were made in the new selections, you can return to the ROUTING Page to correct and re-apply them.</p>
Cancel	<p>Cancels all changes you have made on the ROUTING Page, reverting the page to its previously saved configuration.</p> <p>Any new selections will be deleted and not be applied.</p>

The WIRELESS Configuration Page

MOTOROLA WR850GP

Basic **LAN** **WAN** **Status** **Filters** **Routing** **Wireless** **Security** **Firmware**

WIRELESS
This page allows you to configure your wireless network.

Wireless Interface:

Network Name (SSID):

Network Type:

AP Isolation:

Wireless Enabled:

Country:

Band:

Channel: Current: 11

Wireless Mode:

802.11g Protection Mode:

Rate:

Basic Rate Set:

Multicast Rate:

Fragmentation Threshold:

RTS Threshold:

DTIM Interval:

Beacon Interval:

Preamble Type:

Maximum Associations:

Frame Bursting:

Performance Enhancement (GP models only):

WMM Support:

No-Acknowledgement:

EDCA AP Parameters:

	CWmin	CWmax	AIFS N	TxOP (b) Limit (microsecond)	TxOP (g) Limit (microsecond)	Admin Forced
Background AC	15	1023	7	0	0	<input type="text" value="Off"/>
Best Effort AC	15	63	3	0	0	<input type="text" value="Off"/>
Video AC	7	15	1	6016	3008	<input type="text" value="Off"/>
Voice AC	3	7	1	3264	1504	<input type="text" value="Off"/>

EDCA Client Parameters:

	CWmin	CWmax	AIFS N	TxOP (b) Limit (microsecond)	TxOP (g) Limit (microsecond)	Admin Forced
Background AC	15	1023	7	0	0	<input type="text" value="Off"/>
Best Effort AC	15	1023	3	0	0	<input type="text" value="Off"/>
Video AC	7	15	2	6016	3008	<input type="text" value="Off"/>
Voice AC	3	7	2	3264	1504	<input type="text" value="Off"/>

Wireless Bridge Operation:

Bridge Link Detection Interval:

Wireless Bridge Restriction Mode:

Recognized Bridges:

Peer MAC Address	Link Status

Wireless MAC Restriction Mode:

Restricted Wireless MAC Addresses:

Authenticated Clients:

MAC Address	Associated	Authorized	WME Link
00:0F:66:1D:F5:99	Yes	No	No

This page allows you to configure the wireless network created by your WR850's built-in wireless access point. You can consider the WIRELESS page as divided into three key sets of options:

1) Wireless Mode / Performance Options: Configuration options tied to establishing wireless connections between the WR850 and client devices on your local network.

Figure 3-9a Top of WIRELESS Page – Wireless Modes / Performance

MOTOROLA WR850GP

Basic **LAN** **WAN** **Status** **Filters** **Routing** **Wireless** **Security** **Firmware**

WIRELESS
This page allows you to configure your wireless network.

Wireless Interface:

Network Name (SSID):

Network Type:

AP Isolation:

Wireless Enabled:

Country:

Band:

Channel: Current 11

Wireless Mode:

802.11g Protection Mode:

Rate:

Basic Rate Set:

Multicast Rate:

Fragmentation Threshold:

RTS Threshold:

DTIM Interval:

Beacon Interval:

Preamble Type:

Maximum Associations:

Frame Bursting:

Performance Enhancement (GP models only):

2) Wireless Quality of Service (WMM™) Options: Configuration options tied to optimizing wireless network performance for multimedia applications. WMM (Wi-Fi Multimedia) is an interoperability standard, sponsored by the Wi-Fi Alliance. It provides multimedia enhancements for Wi-Fi® networks that can improve the user experience for audio, video, and voice applications by prioritizing traffic demands from different applications. More information about WMM can be found in the descriptions of WMM-related configuration options to follow, and on the public web site sponsored by the Wi-Fi Alliance.

Figure 3-9b Middle of WIRELESS Page – Wireless Quality of Service (WMM)

WMM Support:	<input type="button" value="Off"/>					
No-Acknowledgement:	<input type="button" value="Off"/>					
EDCA AP Parameters:	CW/min	CW/max	AIFS N	TXOP(b) Limit (microsecond)	TXOP(a/g) Limit (microsecond)	Admin Forced
Background AC	15	1023	7	0	0	<input type="button" value="Off"/>
Best Effort AC	15	63	3	0	0	<input type="button" value="Off"/>
Video AC	7	15	1	6016	3008	<input type="button" value="Off"/>
Voice AC	3	7	1	3264	1504	<input type="button" value="Off"/>
EDCA Client Parameters:						
Background AC	15	1023	7	0	0	<input type="button" value="Off"/>
Best Effort AC	15	1023	3	0	0	<input type="button" value="Off"/>
Video AC	7	15	2	6016	3008	<input type="button" value="Off"/>
Voice AC	3	7	2	3264	1504	<input type="button" value="Off"/>

3) Wireless Distribution System (WDS) and Access Control Options: Configuration options tied to either configuring the WR850 to extend a wireless network (instead of creating a new one) or controlling access to the wireless network.

Figure 3-9c Bottom of WIRELESS Page – WDS and Access Control

Wireless Bridge Operation:	<input type="text" value="Access Point/Wireless Bridge"/>			
Bridge Link Detection Interval:	<input type="text" value="0"/>			
Wireless Bridge Restriction Mode:	<input type="text" value="Enabled"/>			
Recognized Bridges:	<input type="text" value="Peer MAC Address"/>	<input type="text" value="Link Status"/>		
	<input type="text"/>			
	<input type="text"/>			
	<input type="text"/>			
	<input type="text"/>			
Wireless MAC Restriction Mode:	<input type="text" value="Disabled"/>			
Restricted Wireless MAC Addresses:	<input type="text"/>	<input type="text"/>		
	<input type="text"/>	<input type="text"/>		
	<input type="text"/>	<input type="text"/>		
	<input type="text"/>	<input type="text"/>		
	<input type="text"/>	<input type="text"/>		
	<input type="text"/>	<input type="text"/>		
	<input type="text"/>	<input type="text"/>		
	<input type="text"/>	<input type="text"/>		
Authenticated Clients:	<input type="text" value="MAC Address"/>	<input type="text" value="Associated"/>	<input type="text" value="Authorized"/>	<input type="text" value="WMM Link"/>
	00:0F:66:1D:F5:99	Yes	No	No
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

WIRELESS Page – Commonly Used Configuration Options

The following configuration options are highlighted in **white** on the WIRELESS Page, for easy reference. These fields are the most commonly used or adjusted, in supporting typical uses of the WR850 as a wired/wireless router.

The rest of the configuration options are provided primarily for advanced users.

Field	Description
Network Name (SSID):	<p>Sets the Network Name (also known as SSID, or Service Set Identifier) of the WR850 wireless interface.</p> <p>When a client looks to connect wirelessly to this WR850, this SSID will be the identifier by which they recognize the network.</p> <p>The SSID can be up to 32 alphanumeric characters.</p> <p>FACTORY DEFAULT: motorola + the Wireless MAC address</p>
Channel:	<p>Sets which wireless channel to use (e.g., when <i>Country</i> is set to the United States, the available channels are numbered 1 through 11). If you encounter poor wireless performance due to interference, you can switch the channel.</p> <p>FACTORY DEFAULT: 11</p>

WIRELESS Page – All Configuration Options

Options related to: ESTABLISHING YOUR WIRELESS NETWORK

Wireless Interface:

Network Name (SSID):

Network Type:

AP Isolation:

Field	Description
Wireless Interface: (ADVANCED)	<p>Sets the wireless interface to be configured.</p> <p>NOTE: <i>The WR850 currently offers only one interface; future versions of WR850 hardware may include multiple wireless interfaces.</i></p> <p>FACTORY DEFAULT: Built-in WR850 Wireless MAC address, as printed on the product label as “Wireless MAC”.</p>
Network Name (SSID):	<p>Sets the Network Name (also known as SSID, or Service Set Identifier) of this wireless interface.</p> <p>When a client looks to connect wirelessly to this WR850, this SSID will be the identifier by which they recognize the network.</p> <p>The SSID can be up to 32 alphanumeric characters.</p> <p>FACTORY DEFAULT: motorola + the Wireless MAC address</p>
Network Type: (ADVANCED)	<p>Sets whether or not the WR850 openly broadcasts its SSID over the wireless network, for clients to identify in passive scans.</p> <ul style="list-style-type: none"> • Selecting Open enables SSID broadcasting and responses to passive scans by clients. • Selecting Closed disables SSID broadcasting; the WR850 will respond only to active scans by clients. <p>FACTORY DEFAULT: Open</p>
AP Isolation: (ADVANCED)	<p>Sets whether or not associated wireless clients will be able to communicate with each other through the access point.</p> <ul style="list-style-type: none"> • Selecting On disables client-to-client communications. <p>FACTORY DEFAULT: Off</p>

Options related to: ENSURING INTEROPERABILITY WITH WIRELESS DEVICES

Wireless Enabled: Yes

Country: UNITED STATES

Band: 802.11g (2.4 GHz)

Channel: 11 Current: 11

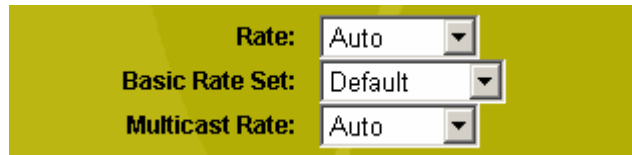
Wireless Mode: Compatibility

802.11g Protection Mode: Auto

Field	Description
Wireless Enabled: (ADVANCED)	Enables wireless operation on this interface. Select Yes or No . FACTORY DEFAULT: Yes
Country:	Identifies the country name in which the wireless operation parameters are set to comply with. Currently United States is the only option. FACTORY DEFAULT: United States
Band:	Sets which wireless radio band to use. 802.11g is the only option. <i>NOTE:</i> The 2.4 GHz radio band supports both 802.11g and 802.11b devices, unless you disable backward compatibility through the setting of the Wireless Mode below. FACTORY DEFAULT: 802.11g (2.4 GHz)
Channel:	Sets which wireless channel to use (e.g., when <i>Country</i> (above) is set to the United States, the available channels are numbered 1 through 11). If you encounter poor wireless performance due to interference, you can switch the channel. FACTORY DEFAULT: 11
Wireless Mode: (ADVANCED)	Sets the compatibility mode for the wireless interface. You should select the setting of this option based on the types of wireless clients you are planning to use. <ul style="list-style-type: none"> • Select Compatibility if using the WR850 with both 802.11g and 802.11b clients. • Select Performance for best service if using the WR850 only with 802.11g clients (with no 802.11b “neighbors”). • Select LRS if you are experiencing particular difficulty with 802.11b clients. • Select 802.11b only for best service if using the WR850 only with 802.11b clients. FACTORY DEFAULT: Compatibility

Field	Description
802.11g Protection Mode: (ADVANCED)	<p>When 802.11g and 802.11b devices are used together, the wireless performance of 802.11g devices is typically reduced, as part of enabling the system to be backward compatible.</p> <p>The WR850 is equipped to be able to minimize this performance impact on 802.11g devices in a “mixed” environment.</p> <ul style="list-style-type: none"> • Selecting Auto enables this feature. • Selecting Off disables this feature. <p>NOTE: Selecting Auto is recommended if Wireless Mode (above) is set to either Compatibility or LRS.</p> <p>FACTORY DEFAULT: Auto</p>

Options related to: CUSTOMIZING WIRELESS DATA THROUGHPUT



Rate: Auto

Basic Rate Set: Default

Multicast Rate: Auto

Field	Description
Rate: (ADVANCED)	<p>Sets a specific value for the wireless data rate, if desired.</p> <p>You can select a specific data rate from those in the pull-down list, to force connections to be made only when a certain level of performance can be guaranteed.</p> <p>NOTE: If you are using 802.11b clients, you should not select a Rate greater than 11 Mbps, since this is the maximum data rate for 802.11b clients.</p> <p>Your WR850 can automatically adjust the wireless data rate when communicating with clients, in order to maximize the data rate under varying conditions (range, interference, etc.). Select Auto to enable this feature.</p> <p>FACTORY DEFAULT: Auto</p>
Basic Rate Set: (ADVANCED)	<p>Sets how the WR850 advise wireless clients of the data rate at which to communicate.</p> <ul style="list-style-type: none"> • Select Default for compatibility with both 802.11g and 802.11b clients. • Select All for compatibility with all wireless clients. • Select 1 & 2 Mbps to communicate at minimum rates. <p>FACTORY DEFAULT: Default</p>

Field	Description
Multicast Rate: (ADVANCED)	<p>Sets a specific value for the wireless data rate for multicast/broadcast applications, since these applications can absorb network capacity more quickly.</p> <p>You can select a specific data rate from those in the pull-down list, to force multicasts or broadcasts to fall within a certain capacity limit.</p> <p>Your WR850 can automatically adjust the wireless data rate when communicating with clients, in order to optimize performance for clients. Select Auto to enable this feature.</p> <p>FACTORY DEFAULT: Auto</p>

Options related to: OPTIMIZING WIRELESS OPERATION FOR YOUR ENVIRONMENT

Fragmentation Threshold:

RTS Threshold:

DTIM Interval:

Beacon Interval:

Preamble Type:

Maximum Associations:

Field	Description
Fragmentation Threshold: (ADVANCED)	<p>Data communicated over the wireless network is fragmented and sent in “packets” instead of all at once. This is part of the scheme by which the wireless channel is shared among multiple users.</p> <p>The fragmentation threshold sets the size of these “packets” in bytes. The entered value must be between 256 and 2346.</p> <p>FACTORY DEFAULT: 2346</p>
RTS Threshold: (ADVANCED)	<p>Sets the packet size, in bytes, for Request to Send (RTS) messages sent by the WR850.</p> <p>The entered value must be between 0 and 2347.</p> <p>FACTORY DEFAULT: 2347</p>
DTIM Interval: (ADVANCED)	<p>Sets the time period to communicate within a Delivery Traffic Indication Message (DTIM), in multiples of <i>Beacon Intervals</i> (see below). A DTIM informs clients when to expect broadcast and multicast messages (allowing them to “power save” in between).</p> <p>The entered value must be between 1 and 255.</p> <p>FACTORY DEFAULT: 3</p>

Field	Description
Beacon Interval: (ADVANCED)	<p>The WR850 will transmit beacons in order to keep the wireless network synchronized. The <i>Beacon Interval</i> sets the length of time in between beacons in Time Units (TU).</p> <p>The entered value must be between 1 and 9999.</p> <p>FACTORY DEFAULT: 100</p>
Preamble Type: (ADVANCED)	<p>Preambles are built into wireless communications over the network to ensure proper delivery of data. A short preamble can free up more capacity for useful data, but all devices on your wireless network must support them.</p> <p>Select Long or Short.</p> <p>FACTORY DEFAULT: Long</p>
Maximum Associations: (ADVANCED)	<p>Sets a limit on the number of wireless clients that can be simultaneously associated with the WR850.</p> <p>The entered value must be between 1 and 256.</p> <p>FACTORY DEFAULT: 128</p>

Options related to: BOOSTING WIRELESS PERFORMANCE
(with compatible clients)

Frame Bursting:

Performance Enhancement (GP models only):

Field	Description
Frame Bursting: (ADVANCED)	<p>The WR850 can improve wireless network efficiency by encapsulating more useful data packets within transmissions over a given time period, reducing the transmission “overhead.”</p> <p>To function, this Frame Bursting feature must also be supported and enabled in associated wireless clients.</p> <ul style="list-style-type: none"> Selecting On engages Frame Bursting. Selecting Off disengages Frame Bursting. <p>FACTORY DEFAULT: Off on WR850G, On on WR850GP</p>
Performance Enhancement: (WR850GP only) (ADVANCED)	<p>The WR850GP can boost wireless performance by up to 35% when used with Performance Enhanced clients.</p> <p>Performance Enhanced clients include those equipped with WN825GP Wireless Notebook Adapters or WPCI810GP Wireless PCI Adapters.</p> <ul style="list-style-type: none"> Select On engages the Performance Enhancement. <p>(continued on next page)</p>

Field	Description
Performance Enhancement: (WR850GP only) <i>(continued)</i>	<ul style="list-style-type: none"> Select Off disengages the Performance Enhancement. <p>NOTES:</p> <ol style="list-style-type: none"> The Performance Enhancement can be On even if one or more clients are not Performance Enhanced, but the performance boost will not be seen while those devices are associated with the WR850GP. When using the Performance Enhancement, the Wireless Mode (above) should be Compatibility or Performance. It is recommended to enable Frame Bursting (above) when enabling the Performance Enhancement. The Performance Enhancement is not compatible with WMM Support (below). To enable WMM features, you will need to set Performance Enhancement to Off. <p>FACTORY DEFAULT: On on WR850GP Off (greyed out and unchangeable) on WR850G</p>

Options related to: OPTIMIZING WIRELESS PERFORMANCE FOR MULTIMEDIA
(Voice and/or Video)

WMM Support:	<input type="button" value="Off"/>					
No-Acknowledgement:	<input type="button" value="Off"/>					
EDCA AP Parameters:	CWmin	CWmax	AIFS N	TxOP(b) Limit (microsecond)	TxOP(a/g) Limit (microsecond)	Admin Forced
Background AC	15	1023	7	0	0	<input type="button" value="Off"/>
Best Effort AC	15	63	3	0	0	<input type="button" value="Off"/>
Video AC	7	15	1	6016	3008	<input type="button" value="Off"/>
Voice AC	3	7	1	3264	1504	<input type="button" value="Off"/>
EDCA Client Parameters:						
Background AC	15	1023	7	0	0	<input type="button" value="Off"/>
Best Effort AC	15	1023	3	0	0	<input type="button" value="Off"/>
Video AC	7	15	2	6016	3008	<input type="button" value="Off"/>
Voice AC	3	7	2	3264	1504	<input type="button" value="Off"/>

Field	Description
WMM Support: (ADVANCED)	<p>Enables support for Wi-Fi Multimedia (WMM) features, which optimize multimedia (e.g., voice, video) sharing over the network.</p> <ul style="list-style-type: none"> Selecting On engages WMM features. Selecting Off disengages WMM features. <p>NOTE: To enable WMM Support, Performance Enhancement (above) must be Off.</p> <p>FACTORY DEFAULT: Off</p>

Field	Description
No-Acknowledgement: (ADVANCED)	<p>Enables No-Acknowledgment operation in WMM, entrusting that the WR850 and clients can share prioritization settings without the need to transmit acknowledgement messages.</p> <p>Disabling acknowledgement messages can free up wireless network capacity but can increase opportunities for errors if strong wireless connections are not established between the WR850 and all WMM-enabled clients.</p> <ul style="list-style-type: none"> • Selecting On entrusts that prioritization can occur without acknowledgement messages. • Selecting Off mandates acknowledgement messages. <p>FACTORY DEFAULT: Off</p>
EDCA AP and Client Parameters: (ADVANCED)	<p>WMM uses a protocol called Enhanced Distributed Channel Access (EDCA) to prioritize traffic on the wireless network. EDCA requires that wireless devices assign each intended transmission a priority, within an Access Category (AC).</p> <p>WMM defines 4 Access Categories:</p> <ul style="list-style-type: none"> • Voice, to give voice traffic the highest priority, since it has the least tolerance for delays and/or loss of data. • Video, to give video a higher priority than other traffic, and optimize real-time video display. • Best Effort, for legacy devices, and/or any other traffic sensitive to delays (e.g., general Internet surfing). • Background, for lowest priority traffic with limited sensitivity to delays (e.g., printing). <p>EDCA manages queues of transmissions within each of these ACs, allocating “slots” of time (or “transmit opportunities”) to each, based on three prioritization settings, set per AC:</p> <ul style="list-style-type: none"> • Arbitrary Inter-Frame Space Number (AIFSN), a minimum number of “slots” a transmission will wait in between transmission opportunities. • Contention Window (CW), a minimum and maximum number of “slots” randomly added to the AIFSN, in order to minimize conflicts between transmissions. • Transmit Opportunity Limit (TXOP limit), the length of time allocated to a transmission once it reaches the top of a queue. For example, video is typically given larger TXOP limits because it is more data-intensive. <p>The WR850 manages EDCA prioritization across the network.</p> <p><i>(continued on next page)</i></p>

Field	Description
EDCA AP and Client Parameters: (continued)	<p>Configuration settings are available to individually adjust EDCA parameters for WR850 transmissions (EDCA AP parameters) and for client device transmissions (EDCA Client parameters).</p> <p>You can set, left to right for each Access Category, the following EDCA parameters:</p> <ul style="list-style-type: none"> • a minimum CW (in slots) • a maximum CW (in slots) • the AISFN (in slots) • a TXOP Limit (b) for 11Mbps 802.11b operation (in microseconds) • a separate TXOP Limit (a/g) for 54Mbps 802.11g operation, since more capacity is available (in microseconds) <p><i>[this last field references 802.11a as well, per WMM standards, since 802.11a is also a 54Mbps wireless technology]</i></p> <p>You can selectively enable and disable specific EDCA parameter settings, on an AC by AC basis, by selecting On or Off in the <i>Admin Forced</i> dialog box at the end of each row.</p> <p>FACTORY DEFAULTS: All settings Off</p>

Options related to: CONFIGURING THE WR850 AS A WIRELESS BRIDGE
(to extend an existing wireless network)

Field	Description
Wireless Bridge Operation: (ADVANCED)	<p>In a typical wireless network configuration, the WR850 serves as wireless access point for clients. However, using built-in Wireless Distribution System (WDS) functionality, the WR850 can be used as a wireless bridge, specifically communicating with other bridges (and/or access points) to create a larger network.</p> <p><i>(continued on next page)</i></p>

Field	Description
Wireless Bridge Operation: <i>(continued)</i>	<p>Sets your wireless interface to operate as an Access Point/Wireless Bridge rather than a Wireless Bridge Only. Wireless bridge operation (also known as Wireless Distribution System or WDS functionality) enables wireless communication only with other wireless bridges to build a larger wireless network.</p> <ul style="list-style-type: none"> • Selecting Access Point/Wireless Bridge retains the WR850's capability to support associations with wireless clients. • Selecting Wireless Bridge Only configures the WR850 to specifically communicate with other wireless bridges and/or access points. <p><i>NOTE:</i> For WDS bridge-to-bridge links to operate properly, ensure that you match wireless security parameters between wireless bridges and access points.</p> <p><i>NOTE:</i> When using Wireless Bridge Only operation, the Performance Enhancement (above) should be Off.</p> <p>FACTORY DEFAULT: Access Point</p>
Bridge Link Detection Interval: <i>(ADVANCED)</i>	<p>Wireless bridges periodically check for other bridges with which to connect. This field sets this bridge link detection interval in seconds.</p> <p>To disable this detection altogether, either leave this field blank or set the value to zero.</p> <p>FACTORY DEFAULT: 0</p>
Wireless Bridge Restriction Mode: <i>(ADVANCED)</i>	<p>Sets whether or not specific access points are recognized as part of the WDS.</p> <ul style="list-style-type: none"> • Select Enabled to limit WDS connections from those listed under Recognized Bridges. • Select Disabled to accept WDS connection from any access point. <p>FACTORY DEFAULT: Enabled</p>
Recognized Bridges: <i>(ADVANCED)</i>	<p>The access point (AP) needs to know the other AP wireless MAC addresses in order to form one WDS connection. The MAC address format is XX:XX:XX:XX:XX:XX. Even when the Wireless Bridge Restriction Mode is Disabled on this AP, its wireless MAC address must be specified in the Recognized Bridges list of the other AP in order to setup a WDS connection.</p> <p>FACTORY DEFAULT: (blank)</p>

Options related to: RESTRICTING WIRELESS ACCESS TO SPECIFIC USERS

Wireless MAC Restriction Mode: Disabled ▾

Restricted Wireless MAC Addresses:

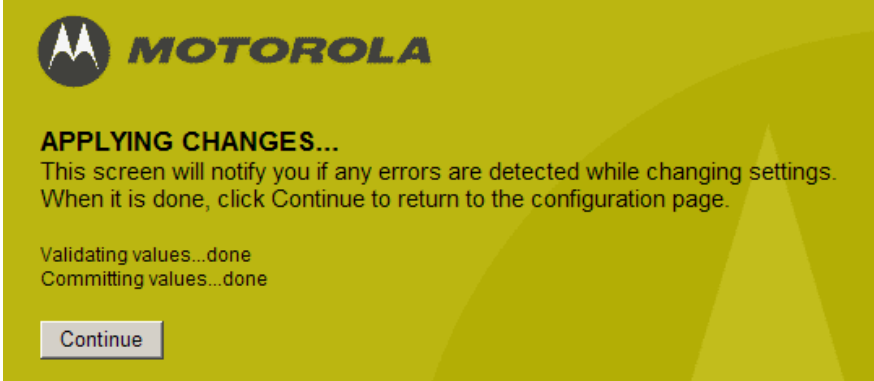
Authenticated Clients:

MAC Address	Associated	Authorized	WME Link
00:0F:66:1D:F5:99	Yes	No	No

Field	Description
Wireless MAC Restriction Mode: (ADVANCED)	<p>Sets restrictions on which wireless clients (specified by wireless MAC address) are allowed to associate with the WR850.</p> <ul style="list-style-type: none"> • Selecting Allow allows access <u>only</u> by those clients identified by the <i>Restricted Wireless MAC Addresses</i>. • Selecting Deny allows access by all clients <u>except</u> those identified by the <i>Restricted Wireless MAC Addresses</i>. • Selecting Disabled suppresses MAC address restrictions. <p>NOTE: While MAC address restrictions can provide a level of security for your wireless network, since MAC addresses can be “spoofed” by hackers, enabling wireless security methods on the <i>SECURITY</i> Page is still recommended.</p> <p>FACTORY DEFAULT: Disabled</p>
Restricted Wireless MAC Addresses: (ADVANCED)	<p>Sets a list of up to sixteen wireless clients (specified by wireless MAC address) for which association is restricted as per the <i>Wireless MAC Restriction Mode</i> above.</p> <p>NOTE: A MAC address has a format of: XX:XX:XX:XX:XX:XX.</p> <p>FACTORY DEFAULT: (blank)</p>
Authenticated Clients: (DISPLAY ONLY)	<p>Shows a list of wireless clients (specified by MAC address) that are “authenticated” (recognized by identification criteria) by the WR850. If “authorization” (allowing access through the WR850 based on authentication) is used, its status is also provided.</p> <p>Additionally, an indication is provided if a connection to this client has been established that can support WMM prioritization. (WME is another acronym commonly used for WMM features.)</p>

WIRELESS Page Action Buttons

At the bottom of the WIRELESS Page, you will see two clickable buttons to process any desired changes to the configuration options.

Button	Purpose
Apply	<p>This button allows you to apply the settings you have selected for WIRELESS Page configuration options.</p> <p>When you click the Apply button, you will see an “Applying Changes” page that shows the status of validating and committing the new selections that have been made.</p>  <p>If no errors were made in the new selections, the prior selections (including any default settings) will be overridden with your new selections. If errors were made in the new selections, you can return to the WIRELESS Page to correct and re-apply them.</p>
Cancel	<p>Cancels all changes you have made on the WIRELESS Page, reverting the page to its previously saved configuration.</p> <p>Any new selections will be deleted and not be applied.</p>

The SECURITY Configuration Page

This page allows you to protect information shared over your wireless network. **It is strongly recommended that at least some level of wireless security be applied to any wireless network.**

Common configuration parameters are highlighted in this section, in order to help you establish a recommended level of wireless security. However, all security options are presented, so that you can match WR850 security settings to the capabilities of the devices with which you will use the WR850.

Figure 3-6 SECURITY Page

MOTOROLA WR850GP

Basic LAN WAN Status Filters Routing Wireless **Security** Firmware

SECURITY
This page allows you to configure security features, to protect information shared over wireless connections.

Wireless Interface:

802.11 Authentication:

802.1X Authentication:

WPA:

WPA2:

WPA2 Pre-authentication:

WPA-PSK:

WPA2-PSK:

WPA Encryption:

WPA Pass Phrase:

Network Key Rotation Interval:

WEP Encryption:

WEP Network Key 1:

WEP Network Key 2:

WEP Network Key 3:

WEP Network Key 4:

Current WEP Network Key Index:

RADIUS Server:

RADIUS Port:

RADIUS Shared Secret:

Network Re-authentication Interval:

You will find that the wireless security settings on the SECURITY page are essentially broken down into enabling two security components on your network:

- **Authentication** methods – means of establishing identification criteria by which wireless clients are recognized (akin to different types of ID cards).

WIRELESS AUTHENTICATION METHODS

- 1) **802.11 Authentication**, which re-uses encryption keys as identification criteria.
- 2) **802.1X Authentication**, which introduces a RADIUS (Remote Authentication Dial-In User Service) authentication server to verify the identity of a client device with a “shared secret” (similar to a password) and dynamically generate an encryption key. *802.1X Authentication can be used with or without 802.11 Authentication.*
- 3) **Wi-Fi® Protected Access (WPA)** authentication, a recent standard issued by the Wi-Fi Alliance, which advocates the use of either 802.1X or a Pre Shared Key (PSK) authentication method, based on enterprise or home wireless use. The PSK method, typically used in home applications, is called **WPA-PSK**. WPA-PSK uses a pass phrase (similar to a password, but not limited to one word) to automatically generate encryption keys, and does not require a RADIUS server.
- 4) **Wi-Fi® Protected Access version 2 (WPA2)** authentication, an updated standard issued by the Wi-Fi Alliance, but still advocating the use of either 802.1X or a PSK authentication method. The updated PSK method is called **WPA2-PSK**. WPA2-PSK, like WPA-PSK, uses a pass phrase to automatically generate encryption keys, and does not require a RADIUS server.

- **Encryption** methods – means of encoding data transmitted over the wireless network, so that only devices with a proper decoder can read that data. Encryption methods use “keys” to encode and decode data.

WIRELESS ENCRYPTION METHODS

- 1) **Wired Equivalent Privacy (WEP)**, which requires the manual entry of a 64-bit or 128-bit encryption key. The same key must be used at both ends of the wireless link. WEP uses this key until it is manually changed, making WEP inherently less secure than other encryption methods. *WEP is the only encryption method that is compatible with 802.11 or 802.1X authentication.*
- 2) **Temporal Key Integrity Protocol (TKIP)**, a more powerful encryption method which periodically changes the encryption key to increase security. *TKIP encryption requires WPA, WPA-PSK, WPA2, or WPA2-PSK authentication.*
- 3) **Advanced Encryption Standard (AES)**, a high-grade encryption method tested to government standards. *AES encryption requires WPA, WPA-PSK, WPA2, or WPA2-PSK authentication.*

Remember that securing your wireless network requires that you use the same authentication and encryption methods in the WR850 and in the devices with which it will communicate.

If you have a set of wireless devices with varying authentication and/or encryption capabilities, the WR850 can concurrently support multiple methods accommodating some combinations.

SECURITY Page – Recommended Configuration Options

The following configuration options are highlighted in **white** on the SECURITY Page for easy reference. These are the options for which adjustments are recommended in order to establish a new wireless network with quality security measures.

These options establish security as per Wi-Fi Protected Access (WPA) standards.

If you intend to use wireless devices with the WR850 that are not capable of supporting WPA, then you should establish security measures that are backward compatible with the capabilities of those devices.

Field	Description
WPA-PSK: (RECOMMENDED)	<p>Enables WPA-PSK (Pre-Shared Key) authentication. Requires a WPA Pass Phrase. It is recommended to enable WPA-PSK and WPA2-PSK concurrently to support clients with mixed capabilities.</p> <ul style="list-style-type: none"> Selecting Enabled engages WPA-PSK. Selecting Disabled disengages WPA-PSK. <p>NOTES:</p> <ol style="list-style-type: none"> WPA-PSK requires a WPA Encryption method (below), and a WPA Pass Phrase (below). WPA-PSK does not require the use of a RADIUS server. WPA-PSK and WPA2-PSK (below) can be enabled concurrently, to support devices with mixed capabilities. WPA-PSK can be used concurrently with WEP Encryption, if needed for backward compatibility. WEP Encryption is enabled separately from WPA Encryption (below). <p>FACTORY DEFAULT: Disabled</p> <p>✓ RECOMMENDED SETTING: Enabled</p>
WPA2-PSK: (RECOMMENDED)	<p>Enables WPA2-PSK (Pre-Shared Key) authentication. Requires a WPA Pass Phrase. It is recommended to enable WPA-PSK and WPA2-PSK concurrently to support clients with mixed capabilities.</p> <ul style="list-style-type: none"> Selecting Enabled engages WPA2-PSK. Selecting Disabled disengages WPA2-PSK. <p>NOTES:</p> <ol style="list-style-type: none"> WPA2-PSK requires a WPA Encryption method (below), and a WPA Pass Phrase (below). WPA2-PSK does not require the use of a RADIUS server. <p>(continued on next page)</p>

Field	Description
WPA2-PSK: (continued)	<p>3) WPA2-PSK and WPA-PSK (above) can be enabled concurrently, to support devices with mixed capabilities.</p> <p>4) WPA2-PSK can be used concurrently with WEP Encryption, if needed for backward compatibility. WEP Encryption is enabled separately from WPA Encryption (below).</p> <p>FACTORY DEFAULT: Disabled</p> <p>✓ RECOMMENDED SETTING: Enabled</p>
WPA Encryption: (RECOMMENDED)	<p>Sets the encryption method(s) to be used with WPA, WPA2, WPA-PSK, or WPA2-PSK authentication.</p> <ul style="list-style-type: none"> • Selecting TKIP engages Temporal Key Integrity Protocol. • Selecting AES engages Advanced Encryption Standard. • Selecting TKIP + AES allows the WR850 to support a mix of devices using these two encryption methods. <p>NOTE: WPA Encryption is greyed out and unchangeable unless WPA, WPA2, WPA-PSK, or WPA2-PSK is Enabled.</p> <p>FACTORY DEFAULT: TKIP</p> <p>✓ RECOMMENDED SETTING: TKIP + AES</p>
WPA Pass Phrase: (RECOMMENDED)	<p>Sets the pass phrase (or Pre-Shared Key) that will be used to generate encryption keys, with WPA-PSK or WPA2-PSK authentication. The entered pass phrase must be:</p> <ul style="list-style-type: none"> • between 8 and 63 alphanumeric characters, or • exactly 64 hexadecimal digits (0-9, A-F). <p>A WPA Pass Phrase of at least 20 characters is strongly recommended, for stronger security.</p> <p>For security reasons, the pass phrase is not immediately readable, while it is being entered. After you apply your changes to the SECURITY Page (i.e., by clicking the <i>Apply</i> button at the bottom of the page), you can use the <i>Show</i> button to the right of this field to review the entered value.</p> <p>This will allow you to recall your WPA Pass Phrase and enter it into the wireless devices with which the WR850 will communicate.</p> <p>NOTE: A WPA Pass Phrase cannot be entered unless WPA-PSK or WPA2-PSK is Enabled.</p> <p>FACTORY DEFAULT: (blank)</p> <p>✓ RECOMMENDED SETTING: A Pass Phrase of at least 20 characters</p>

SECURITY Page – All Configuration Options

Options related to: SELECTING WIRELESS AUTHENTICATION METHODS

Field	Description
Wireless Interface: (ADVANCED)	Sets the wireless interface to be configured. <p>NOTE: The WR850 currently offers only one interface; future versions of WR850 hardware may include multiple wireless interfaces. This interface will be the same as displayed on the WIRELESS Page.</p> <p>FACTORY DEFAULT: Built-in WR850 Wireless MAC address, as printed on the product label as “Wireless MAC”.</p>
802.11 Authentication: (ADVANCED)	Enables a “shared” authentication method, whereby encryption keys are re-used as identification criteria for wireless clients. This “shared” authentication assumes that Wired Equivalent Privacy (WEP) encryption is used, and that WEP encryption keys have previously been shared between the client and access point. <ul style="list-style-type: none"> • Selecting Open disables 802.11 authentication. • Selecting Shared enables 802.11 authentication. <p>NOTE: Selecting Shared will force all configuration options related to WPA authentication (below) to Disabled.</p> <p>NOTE: Selecting Shared requires WEP Encryption to be enabled below, to allow re-use of the encryption keys for identification.</p> <p>FACTORY DEFAULT: Open</p>
802.1X Authentication: (ADVANCED)	Enables the use of the WR850 with a RADIUS (Remote Authentication Dial-In User Service) authentication server, without engaging WPA. During the authentication process, a RADIUS server verifies identities of client devices with a “shared secret” (similar to a password), and dynamically generates encryption keys. <p>802.1X authentication is best enabled only if using the WR850 with devices that are not capable of supporting WPA.</p> <p style="text-align: right;">(continued on next page)</p>

Field	Description
802.1X Authentication: (continued)	<ul style="list-style-type: none"> Selecting Enabled sets the WR850 to work with a RADIUS server, <i>without engaging WPA or WPA2 (below)</i>. Selecting Disabled sets the WR850 to work with a RADIUS server <i>only if used with WPA or WPA2 (below)</i>. <p>NOTE: <i>802.1X Authentication</i> requires you to complete the configuration options related to “Setting Up Compatibility with a RADIUS Server”.</p> <p>NOTE: <i>802.1X Authentication</i> can be enabled concurrently with WPA or WPA2, but the WR850 can only support one RADIUS server on the network.</p> <p>FACTORY DEFAULT: Disabled</p>
WPA: (ADVANCED)	<p>Enables 802.1X-based WPA authentication with a RADIUS server.</p> <ul style="list-style-type: none"> Selecting Enabled engages WPA. Selecting Disabled disengages WPA. <p>NOTE: <i>WPA</i> requires you to complete the configuration options related to “Setting Up Compatibility with a RADIUS Server”.</p> <p>NOTE: <i>WPA</i> requires a WPA Encryption method (below).</p> <p>FACTORY DEFAULT: Disabled</p>
WPA2: (ADVANCED)	<p>Enables 802.1X-based WPA2 authentication with a RADIUS server.</p> <ul style="list-style-type: none"> Selecting Enabled engages WPA2. Selecting Disabled disengages WPA2. <p>NOTE: <i>WPA2</i> requires you to complete the configuration options related to “Setting Up Compatibility with a RADIUS Server”.</p> <p>NOTE: <i>WPA2</i> requires a WPA Encryption method (below).</p> <p>FACTORY DEFAULT: Disabled</p>
WPA2 Pre-authentication: (ADVANCED)	<p>Enables clients to authenticate, in advance, with multiple access points, in order to roam quickly among access points.</p> <ul style="list-style-type: none"> Selecting Enabled allows clients to pre-authenticate with the WR850. Selecting Disabled does not allow clients to pre-authenticate with the WR850. <p>NOTE: <i>WPA2 Pre-authentication</i> is greyed out and unchangeable unless WPA2 (above) is Enabled.</p> <p>FACTORY DEFAULT: Disabled</p>

Field	Description
WPA-PSK: (RECOMMENDED)	<p>Enables Wi-Fi Protected Access (WPA) authentication using the Pre-Shared Key (PSK) method.</p> <ul style="list-style-type: none"> • Selecting Enabled engages WPA-PSK. • Selecting Disabled disengages WPA-PSK. <p>NOTES:</p> <ol style="list-style-type: none"> 1) WPA-PSK requires a WPA Encryption method (below), and a WPA Pass Phrase (below). 2) WPA-PSK does not require the use of a RADIUS server. 3) WPA-PSK and WPA2-PSK (below) can be enabled concurrently, to support devices with mixed capabilities. 4) WPA-PSK can be used concurrently with WEP Encryption, if needed for backward compatibility. WEP Encryption is enabled separately from WPA Encryption (below). <p>FACTORY DEFAULT: Disabled</p>
WPA2-PSK: (RECOMMENDED)	<p>Enables Wi-Fi Protected Access version 2 (WPA2) authentication using the Pre-Shared Key (PSK) method.</p> <ul style="list-style-type: none"> • Selecting Enabled engages WPA2-PSK. • Selecting Disabled disengages WPA2-PSK. <p>NOTES:</p> <ol style="list-style-type: none"> 1) WPA2-PSK requires a WPA Encryption method (below), and a WPA Pass Phrase (below). 2) WPA2-PSK does not require the use of a RADIUS server. 3) WPA2-PSK and WPA-PSK (above) can be enabled concurrently, to support devices with mixed capabilities. 4) WPA2-PSK can be used concurrently with WEP Encryption, if needed for backward compatibility. WEP Encryption is enabled separately from WPA Encryption (below). <p>FACTORY DEFAULT: Disabled</p>

Options related to: ENABLING WIRELESS ENCRYPTION METHODS

WPA Encryption:

WPA Pass Phrase:

Network Key Rotation Interval:

WEP Encryption:

WEP Network Key 1:

WEP Network Key 2:

WEP Network Key 3:

WEP Network Key 4:

Current WEP Network Key Index:

Field	Description
WPA Encryption: (RECOMMENDED)	<p>Sets the encryption method(s) to be used with WPA, WPA2, WPA-PSK, or WPA2-PSK authentication.</p> <ul style="list-style-type: none"> • Selecting TKIP engages Temporal Key Integrity Protocol. • Selecting AES engages Advanced Encryption Standard. • Selecting TKIP + AES allows the WR850 to support a mix of devices using these two encryption methods. <p><i>NOTE:</i> <i>WPA Encryption is greyed out and unchangeable unless WPA, WPA2, WPA-PSK, or WPA2-PSK is Enabled.</i></p> <p>FACTORY DEFAULT: TKIP</p>
WPA Pass Phrase: (RECOMMENDED)	<p>Sets the pass phrase (or Pre-Shared Key) that will be used to generate encryption keys, with WPA-PSK or WPA2-PSK authentication. The entered pass phrase must be:</p> <ul style="list-style-type: none"> • between 8 and 63 alphanumeric characters, or • exactly 64 hexadecimal digits (0-9, A-F). <p>A WPA Pass Phrase of at least 20 characters is strongly recommended, for stronger security.</p> <p>For security reasons, the pass phrase is not immediately readable while it is being entered. After you apply your changes to the SECURITY Page (i.e., by clicking the <i>Apply</i> button at the bottom of the page), you can use the <i>Show</i> button to the right of this field to review the entered value.</p> <p>This will allow you to recall your WPA Pass Phrase and enter it into the wireless devices with which the WR850 will communicate.</p> <p><i>NOTE:</i> <i>A WPA Pass Phrase cannot be entered unless WPA-PSK or WPA2-PSK is Enabled.</i></p> <p>FACTORY DEFAULT: (blank)</p>

Field	Description
Network Key Rotation Interval: (ADVANCED)	<p>With WPA encryption methods, the WR850 can issue clients new encryption keys for multicast and broadcast packets on periodic basis. This field sets that periodic interval in seconds. Leave this field blank, or set the value to zero, to disable this periodic update.</p> <p>NOTE: <i>Network Key Rotation Interval</i> is greyed out and unchangeable unless WPA, WPA2, WPA-PSK, or WPA2-PSK is Enabled.</p> <p>FACTORY DEFAULT: 86400</p>
WEP Encryption: (ADVANCED)	<p>Enables Wired Equivalent Privacy (WEP) encryption.</p> <ul style="list-style-type: none"> • Selecting Enabled engages WEP. • Selecting Disabled disengages WEP. <p>NOTE: <i>WEP Encryption</i> requires the entry of at least one WEP Network Key (below).</p> <p>FACTORY DEFAULT: Disabled</p>
WEP Network Keys 1-4: (ADVANCED)	<p>Sets up to four specific encryption keys which be used with WEP encryption. You can enter 64-bit keys or 128-bit keys:</p> <ul style="list-style-type: none"> • <i>64-bit keys</i> must be made up of either 5 case-sensitive ASCII characters or 10 hexadecimal digits (0-9, A-F). • <i>128-bit keys</i> must be made up of either 13 case-sensitive ASCII characters or 26 hexadecimal digits (0-9, A-F). <p>NOTES:</p> <ol style="list-style-type: none"> 1) You can only enter WEP Network Keys if WEP Encryption (above) is Enabled. 2) Do not enter simple patters of numbers (e.g., all zeroes) as WEP Network Keys. These keys would not be secure. 3) WEP Network Keys need not be entered if 802.1X Authentication (above) is Enabled, since the RADIUS server will dynamically generate keys. 4) If WEP Encryption and WPA Encryption (above) are concurrently Enabled, Network Key slots 1 and 4 are reserved for WPA functions and you will only be able to enter WEP Network Keys into slots 2 and 3. <p>FACTORY DEFAULT: (blank)</p>
Current WEP Network Key Index: (ADVANCED)	<p>Sets which WEP Network Key (above) will be used for encryption. Select from 1 to 4.</p> <p>NOTE: If WEP Encryption and WPA Encryption (above) are concurrently Enabled, Network Key slots 1 and 4 are reserved for WPA functions and the Current WEP Network Key Index will only be able to select between 2 and 3.</p> <p>FACTORY DEFAULT: 1</p>

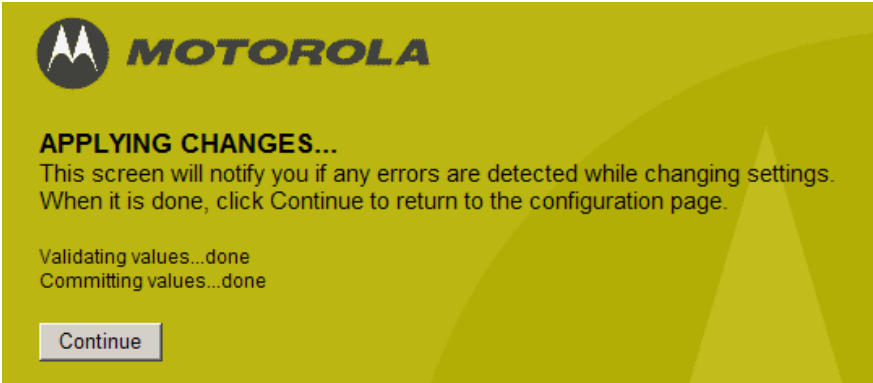
Options related to: SETTING UP COMPATIBILITY WITH A RADIUS SERVER

RADIUS Server:	<input type="text"/>
RADIUS Port:	<input type="text" value="1812"/>
RADIUS Shared Secret:	<input type="text"/>
Network Re-authentication Interval:	<input type="text" value="36000"/>

Field	Description
RADIUS Server: (ADVANCED)	<p>Sets the IP address for the RADIUS server.</p> <p><u>NOTE:</u> A RADIUS Server can only be entered if 802.1X Authentication, WPA, or WPA2 (above) is Enabled.</p> <p>FACTORY DEFAULT: (blank)</p>
RADIUS Port: (ADVANCED)	<p>Sets the port number for the RADIUS server.</p> <p><u>NOTE:</u> RADIUS Port is greyed out and unchangeable unless 802.1X Authentication, WPA, or WPA2 (above) is Enabled.</p> <p>FACTORY DEFAULT: 1812</p>
RADIUS Shared Secret: (ADVANCED)	<p>Sets the password by which authentication can successfully be obtained with the RADIUS server.</p> <p><u>NOTE:</u> A RADIUS Shared Secret can only be entered if 802.1X Authentication, WPA, or WPA2 (above) is Enabled.</p> <p>FACTORY DEFAULT: (blank)</p>
Network Re-authentication Interval: (ADVANCED)	<p>Sets a periodic interval (in seconds), whereby all devices on the wireless network will need to refresh their authentication with the RADIUS server.</p> <p><u>NOTE:</u> Network Re-authentication Interval is greyed out and unchangeable unless 802.1X Authentication, WPA, or WPA2 (above) is Enabled.</p> <p>FACTORY DEFAULT: 36000</p>

SECURITY Page Action Buttons

At the bottom of the SECURITY Page, you will see two clickable buttons to process any desired changes to the configuration options.

Button	Purpose
Apply	<p>This button allows you to apply the settings you have selected for SECURITY Page configuration options.</p> <p>When you click the Apply button, you will see an “Applying Changes” page that shows the status of validating and committing the new selections that have been made.</p>  <p>If no errors were made in the new selections, the prior selections (including any default settings) will be overridden with your new selections. If errors were made in the new selections, you can return to the SECURITY Page to correct and re-apply them.</p>
Cancel	<p>Cancels all changes you have made on the SECURITY Page, reverting the page to its previously saved configuration.</p> <p>Any new selections will be deleted and not be applied.</p>

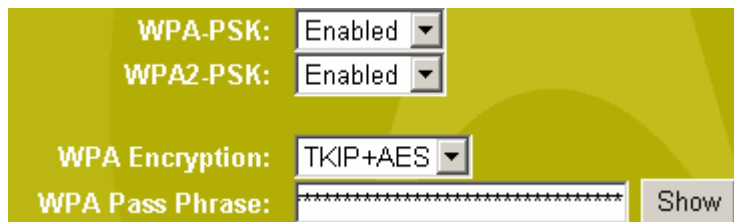
SECURITY Page Example – Matching Settings in the WR850 and Wireless Clients

In order to securely communicate over the wireless network, the WR850 and clients must share common authentication and encryption settings. The following example is provided to demonstrate how you can ensure that settings are appropriately matched in the WR850 and your client devices.

For this example, we assume that:

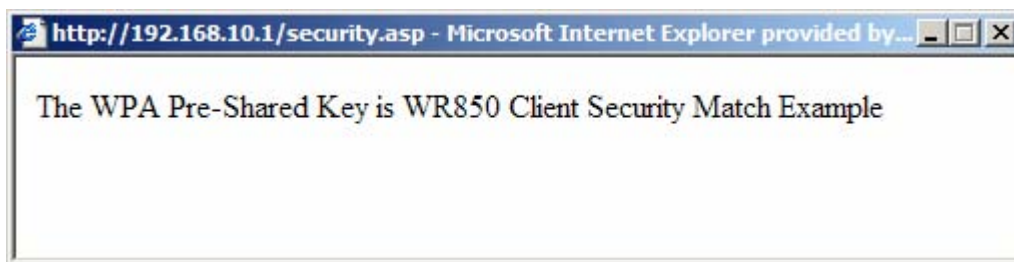
- As per recommendations, you have enabled *WPA-PSK* authentication and *TKIP* encryption in the WR850 with a secure *WPA Pass Phrase*, in this case *WR850 Client Security Match Example*,
- The client is equipped with an Motorola WN825 Wireless Notebook Adapter or a Motorola WPCI810 Wireless PCI Adapter (either of which can support WPA-PSK) and is using the Motorola-provided wireless utility to manage the adapter, and
- You cannot immediately recall the *WPA Pass Phrase*, but have an established wired connection to the WR850, or an already-matched wireless connection, in order to retrieve the *WPA Pass Phrase*.

Step 1: Login to the WR850 Web-based Configuration Utility using your established wired or wireless connection, and navigate to the SECURITY Page to find the *WPA Pass Phrase* configuration option:



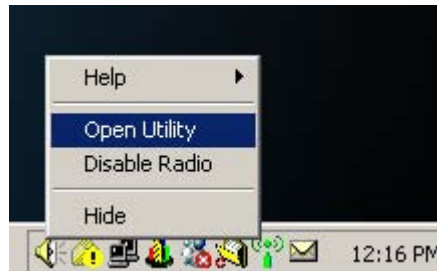
WPA-PSK: Enabled
WPA2-PSK: Enabled
WPA Encryption: TKIP+AES
WPA Pass Phrase: ***** Show

Step 2: Click the *Show* button to the right of the *WPA Pass Phrase*. The following box will be displayed:

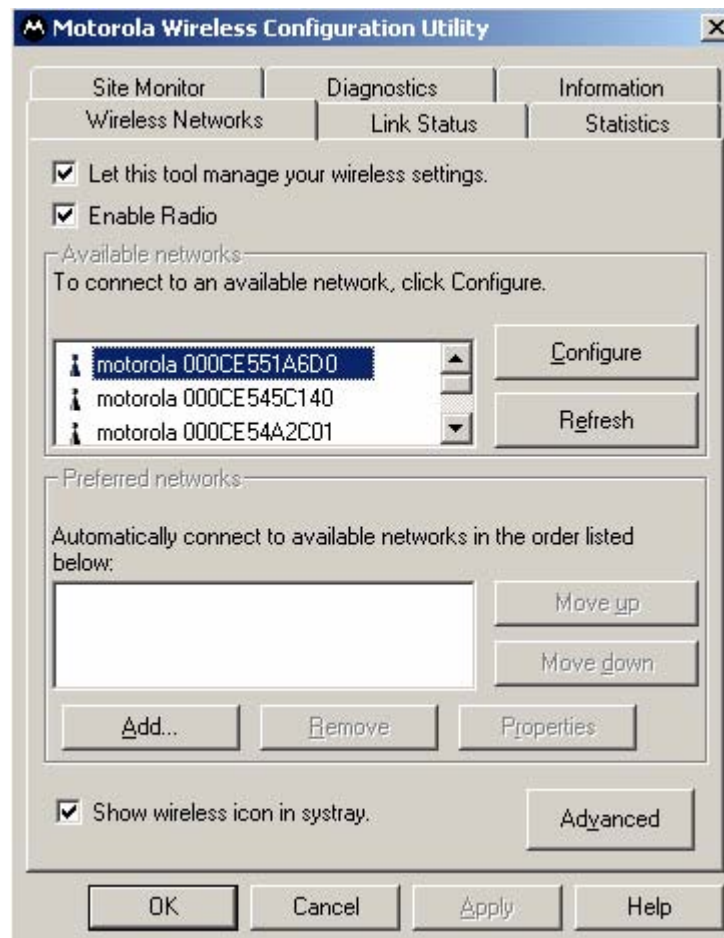


Step 3: Write down in a safe place this WPA Pass Phrase, and move to the PC for which the new secure wireless connection needs to be made.

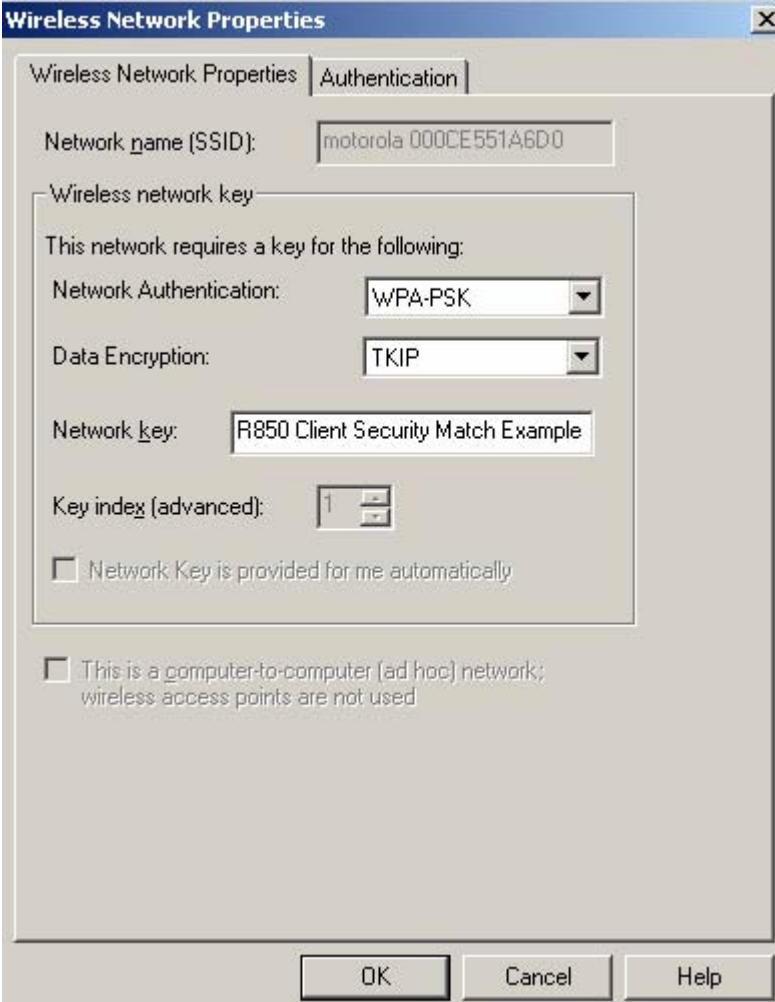
Step 4: Open the client's Motorola Wireless Configuration Utility by right clicking on the wireless icon in the taskbar and selecting *Open Utility*.



Step 5: On the *Wireless Networks* tab, locate the *Network Name (SSID)* for your WR850 in the *Available networks* window and click **Configure**.

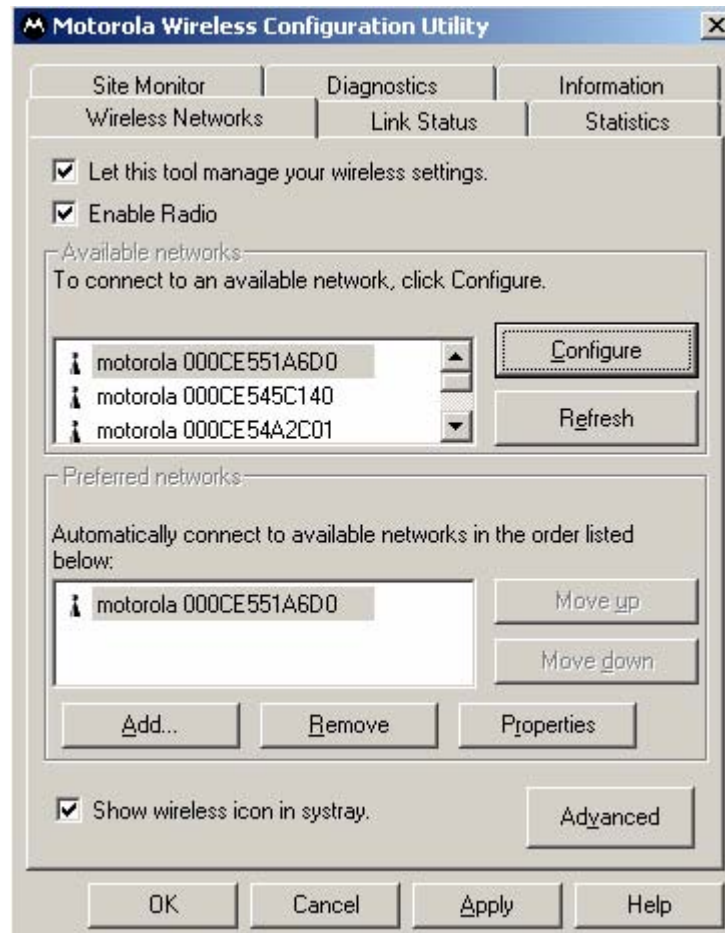


Step 6: On the *Wireless Network Properties* tab, enter the authentication and encryption methods enabled in your WR850 under *Network Authentication* and *Data Encryption* and, in the case of WPA-PSK or WPA2-PSK, enter the WPA Pass Phrase as the *Network Key*. When done, click **OK**.



The image shows a Windows-style dialog box titled "Wireless Network Properties". It has two tabs: "Wireless Network Properties" and "Authentication". The "Authentication" tab is selected. Inside the dialog, there is a text field for "Network name (SSID)" containing "motorola 000CE551A6D0". Below this is a section titled "Wireless network key" which contains the text "This network requires a key for the following:". Underneath, there are two dropdown menus: "Network Authentication" set to "WPA-PSK" and "Data Encryption" set to "TKIP". Below these is a text field for "Network key" containing "R850 Client Security Match Example". There is also a "Key index (advanced)" spinner box set to "1". At the bottom of this section is a checkbox labeled "Network Key is provided for me automatically", which is unchecked. Below the entire section is another checkbox labeled "This is a computer-to-computer (ad hoc) network; wireless access points are not used", which is also unchecked. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

Step 7: Back on the *Wireless Networks* tab, click **Apply** and then **OK**. Your wireless security parameters are now matched, and this client should now be able to securely communicate with the WR850.



The FIRMWARE Configuration Page

This page allows you to update the version of firmware installed in your WR850, as new releases are posted on the Motorola Home Networking Support web site. (You can reach this site by visiting <http://www.motorola.com/homenetworking> and clicking the “Support and Downloads” link.)

Figure 3-6 FIRMWARE Page

FIRMWARE Page Configuration Options

Field	Description
Firmware Version: (DISPLAY ONLY)	Shows the version of firmware currently installed in your WR850.
New Firmware:	<p>Sets a new firmware version to be installed on your WR850.</p> <p>After downloading a new firmware package to your computer, and extracting the firmware (.trx) file from the package, click the <i>Browse ...</i> button to locate that firmware file and select it. Once you select the file, its file name will appear in this field.</p> <p>After confirming that the proper file name is displayed, click the <i>Upgrade</i> button to proceed with the update.</p> <p><i>NOTE:</i> Your WR850 will reboot as part of installing the new firmware version.</p>

Section 4: Troubleshooting

This section details possible solutions to common problems that might occur in using the router.

Contact Us

If you are unable to locate a solution here, please access our website at <http://www.motorola.com/homenetworking> for the latest information. You can also reach us 7 days a week, 24 hours a day at 1-877-466-8646.

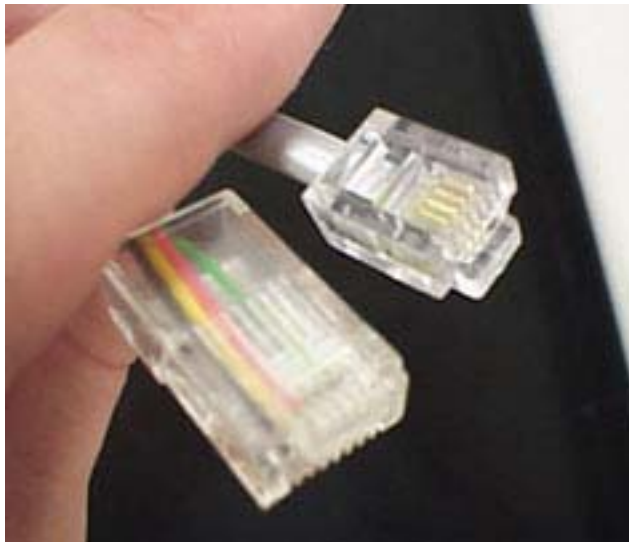
Hardware Solutions

My computer is experiencing difficulty connecting to the wireless network.

- Ensure that your router is powered on and that the Wireless LED is on.
- Ensure that your wireless adapter (PCI card, Notebook or Ethernet adapter) is installed correctly and is active.
- Ensure that your wireless adapter's radio signal is enabled. Review your adapter's documentation for further instructions.
- Ensure that your wireless adapter for your PC and the wireless router have the same security settings that will allow your computer to access the wireless network. Also, verify that the list of *Restricted Wireless MAC Addresses* (on the WIRELESS Page of the Web-based Configuration Utility) is not configured to block your PC. For details on adjusting your security settings, please refer to the descriptions of the WIRELESS and SECURITY Pages in Section 3: Configuration.
- Ensure that your wireless adapter is within range of your router or is not behind an obstruction. For example, metal structures will interfere with the signal, as will 2.4 GHz cordless phones, and microwaves.
- Ensure that your router's antenna is connected and that your PC's wireless adapter antenna is also connected.

My computer is experiencing difficulty in connecting to the router.

- Ensure that all of your cabling connections are firmly connected. This includes the cables from the wall to your modem, between the router and modem, and, if available, from the router to your PC.
- Ensure that your LEDs are not lit **Red** or not at all. For further information about LED descriptions, see Section 1: Overview.
- Ensure that you are using Ethernet cables and not telephone cables between the router and modem or router and PC. See the illustration below. Ethernet cables use a wider RJ-45 style plug using 8 wires where telephone style plugs use the smaller RJ-11 style plug using 4 to 6 wires.



The plug on the left is RJ-45; the plug on the right is RJ-11 – use only RJ-45.

- Ensure that your Ethernet adapter is enabled. To check the status of your adapter, click the monitor icon in the System Tray at the bottom right of your screen.



You can also check the status of the Ethernet adapter by selecting **Control Panel > Network and Dial-Up Connections**.

My broadband modem already uses a built-in router.

Because the two routers will cancel each other out, turn off the NAT function in the modem to enable access for your router. Refer to your modem's documentation for further instructions.

Software Solutions

I would like to test to see if my Internet connection is live.

Use the *ping* command to test the connection. Before attempting, ensure that **Obtain an IP address automatically** has been selected in the computer's settings and that you have an IP address assigned. Refer to Configure Your Computers in Section 2: Installation, for further details.

- 1 Open a command prompt by clicking **Start** and **Run**.
- 2 For Windows 98 and ME, in the Open field, type **command** and press **Enter** or **OK**.
For Windows 2000 and XP, type **cmd**. Or, navigate using your **Start** button to **Programs>Accessories>Command Prompt**.
- 3 In the Command window, type **ipconfig**.
 - You should see an IP address for your network adapter:

```
Ethernet Adapter Local Area Connection:

Connection-specific DNS Suffix.: Example.example.example.com.

IP Address. . . . . : 192.168.10.10

Subnet Mask . . . . . : 255.255.255.0

Default Gateway . . . . . : 192.168.10.1
```

- 4 In the *Command* window, type **ping** followed by the **Router's IP address** and press **Enter**.
 - If you receive a reply (the first word will be *Reply...*), then your computer is connected to the router. Proceed to *Step 4*.
 - If you do NOT receive a reply, repeat steps 1 – 4 on a different computer to verify that the first computer is not the cause of the problem.

Your computer's Default Gateway's IP address may also be your router's IP address. Verify the router's IP address by logging on to the router's Web-based Configuration Utility and reviewing the *IP Address* field on the LAN Page.

- 5 In the Command window, type **ping** followed by your **ISP's default gateway** and press **Enter**.
 - If you receive a reply (For example: *Reply from 216.109.125.72...*), then your connection to the Internet is live.

To verify the ISP default gateway's IP address, log on to the router's Web-based Configuration Utility and verify the *Default Gateway* field on the WAN Page.

- If you do NOT receive a reply, repeat steps 1 - 5 on a different computer to verify that the first computer is not the cause of the problem.

I cannot access the Web-based Configuration Utility for the router.

- Verify your Ethernet connection to the router.
- Verify that the IP address of the PC being used to configure the router is on the same network as the router's configuration IP address.
- The IP address of your network adapter must be on the same network and not a duplicate of any others on the network (for example: 192.168.10.10 and using a subnet mask of 255.255.255.0 can be used to login to the router's default IP address of 192.168.10.1). To adjust the IP address for your PC, refer to Configure Your Computers in Section 2: Installation.
- Verify that you can ping the router on this IP address.
- In the *Command* window, type **ping** and your router's default IP address and press **Enter**.
- If you have changed the factory configured default IP address of the router, you will need to set your network adapter accordingly.
- Verify you are entering the correct URL in the browser. The default is <http://192.168.10.1>. If you think you have changed the IP address used to configure the router and cannot remember it, you must reset the unit back to factory defaults. To do this, press and hold the reset button for more the 5 seconds. This clears the router's user settings, including Username, Password, IP Address, and Subnet mask.
- Once the router is reset to factory default, re-verify the Ethernet connectivity and IP address issues.

How do I extend my wireless network to cover more area?

You need more than one access point with WDS (Wireless Distribution System) enabled to expand your wireless network. For example, if you are running a WR850G or WR850GP, you will need another wireless Access Point (AP), most likely a WA840G or WA840GP (but you can use another WR850G or WR850GP; just ensure that you do not run two DHCP servers at the same time).

Set up both the WR850 and the WA840 with the same wireless SSID, the same channel number, and the same WPA Pass Phrase or WEP keys. It is suggested that you also enable the *Wireless Bridge Restriction Mode* to limit the exposure of your wireless network to outside users. The wireless MAC address of the other AP needs to be added to each AP's list of *Recognized Bridges*, that is, the WA840's wireless MAC address needs to be in the WR850's list of *Recognized Bridges*, and vice versa.

Once enabled, your laptop can now roam between the two APs, thereby extending your wireless network.

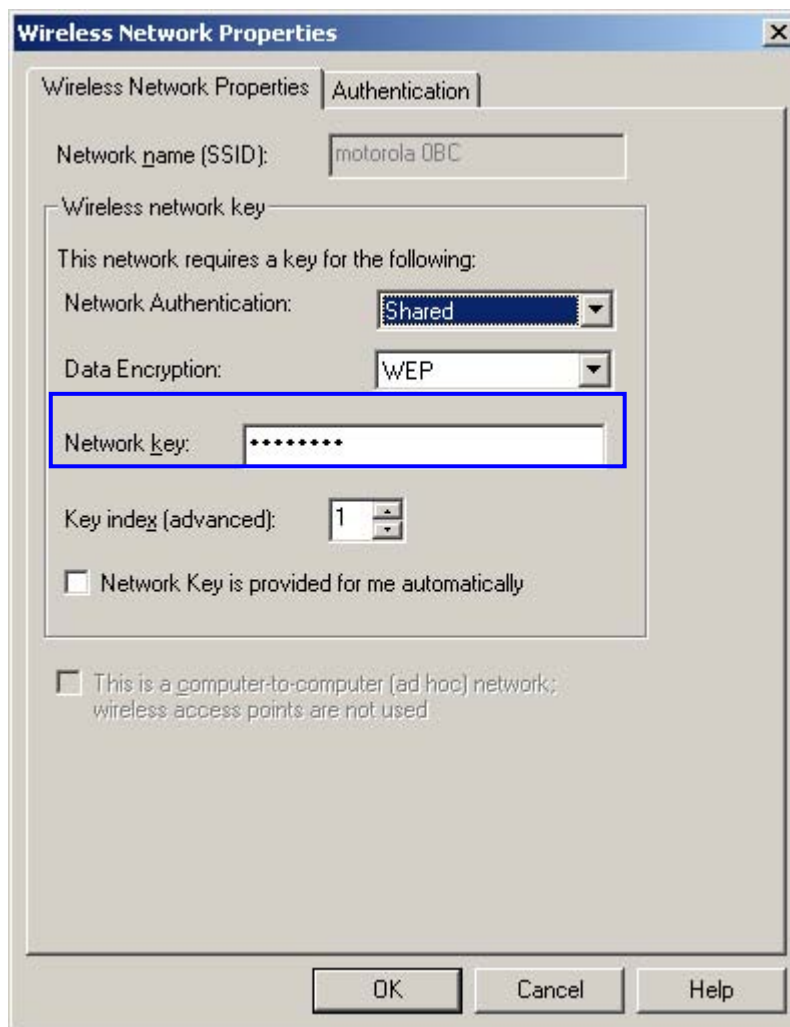
I cannot browse past the first screen of the Web-based Configuration Utility.

Sometimes, especially when upgrading, some leftover files may be in your Internet Cache. Flush your cache and restart your unit to fix. From Internet Explorer's menu, select **Tools > Options** and click **Delete Files** to clear your cache.

How do I match WEP keys between the router and my wireless clients?

Some wireless cards do not support WPA, and in turn cannot accept a WPA Pass Phrase. For compatibility with these clients, *WEP Encryption* must be enabled on the SECURITY Page of the Web-based Configuration Utility, with at least one *WEP Network Key* entered.

Using the utility provided with your wireless client, you must enter the same key that is entered in the WR850. If more than one *WEP Network Key* is entered in the WR850, refer to the *Current WEP Network Key Index* to determine which key to enter in your client device, and then enter the *Current WEP Network Key Index* as the client's Key Index.



Section 5:Glossary

A

Access Point (AP)

A device that provides wireless LAN connectivity to wireless clients (stations). The WR850 acts as a wireless access point.

Adapter

A device or card that connects a computer, printer, or other peripheral device to the network or to some other device. A wireless adapter connects a computer to the wireless LAN.

Address Translation

See *NAT*.

Ad-Hoc Network

A temporary local area network connecting AP clients together, usually just for the duration of the communication session. The clients communicate directly to each other and not through an established, such as through a router. Also known as IBSS (Independent Basic Service Set).

ASCII

The American Standard Code for Information Interchange refers to alphanumeric data for processing and communication compatibility among various devices; normally used for asynchronous transmission.

B

Bandwidth

The transmission capacity of a medium in terms of a range of frequencies. Greater bandwidth indicates the ability to transmit more data over a given period of time.

bps

Bits Per Second

Broadband

A communications medium that can transmit a relatively large amount of data in a given time period.

BSS

Basic Service Set. A configuration of Access Points that communicate with each other without resorting any infrastructure. Also known as Ad-Hoc networks. Also see *ESS*.

C**Client**

In a client/server architecture, a client is a computer that requests files or services such as file transfer, remote login, or printing from the server. On an IEEE 802.11b/g wireless LAN, a client is any host that can communicate with the access point. Also called a CPE. A wireless client is also called a "station." Also see *server*.

Coaxial Cable

A type of cable consisting of a center wire surrounded by insulation and a grounded shield of braided wire. The shield minimizes electrical and radio frequency interference. Coaxial cable has high bandwidth and can support transmission over long distances.

CPE

Customer Premise Equipment: typically computers, printers, etc, that are connected to the gateway at the subscriber location. CPE can be provided by the subscriber or the cable service provider. Also called a client.

Crossover Cable

A crossover cable is a cable that is used to interconnect two computers by "crossing over" (reversing) their respective pin contacts. A crossover cable is sometimes known as a null modem.

D**DDNS**

Dynamic Domain Name System enables you to assign a fixed host and domain name to a dynamic Internet IP address. It is used when you are hosting your own web server, FTP server, or another server behind the router.

Default Gateway

A routing device that forwards traffic not destined to a station within the local subnet.

DHCP

A Dynamic Host Configuration Protocol server dynamically assigns IP addresses to client hosts on an IP network. DHCP eliminates the need to manually assign static IP addresses by “leasing” an IP address and subnet mask to each client. It enables the automatic reuse of unused IP addresses:

The WR850 is simultaneously a DHCP client and a DHCP server.

- A DHCP server at the system headend assigns a public IP address to the WR850.
- The WR850 contains a built-in DHCP server that assigns private IP addresses to clients.

DMZ

DeMilitarized Zone. This service opens one IP address to the Internet, usually for online gaming, and acts as a buffer between the Internet and your network.

DNS

The Domain Name System is the Internet system for converting domain names (like www.motorola.com) to IP addresses. A DNS server contains a table matching domain names such as Internetname.com to IP addresses such as 192.169.9.1. When you access the world-wide web, a DNS server translates the URL displayed on the browser to the destination website IP address. The DNS lookup table is a distributed Internet database; no one DNS server lists all domain name to IP address matches.

Domain Name

A unique name, such as motorola.com, that maps to an IP address. Domain names are typically much easier to remember than are IP addresses. See *DNS*.

Download

To copy a file from one computer to another. You can use the Internet to download files from a server to a computer.

Driver

Software that enables a computer to interact with a network or other device. For example, there are drivers for printers, monitors, graphics adapters, modems, Ethernet, USB, HPNA, and many others.

DSL

Digital Subscriber Line

DSSS

Direct-Sequence Spread Spectrum. DSSS is a transmission technology used in WLAN transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission.

Dynamic IP Address

An IP address that is temporarily leased to a host by a DHCP server. The opposite of *Static IP Address*.

E**ESS**

An Extended Service Set (ESS) is a set of two or more BSSs that form a single subnetwork. See also *BSS*.

Ethernet

The most widely used LAN type, also known as IEEE 802.3. The most common Ethernet networks are 10Base-T, which provide transmission speeds up to 10 Mbps, usually over unshielded, twisted-pair wire terminated with RJ-45 connectors. Fast Ethernet (100Base-T) provides speeds up to 100 Mbps. "Base" means "baseband technology" and "T" means "twisted pair cable."

Each Ethernet port has a physical address called the MAC address. Also see *MAC address*.

Event

A message generated by a device to inform an operator or the network management system that something has occurred.

F**Firewall**

A security software system on the WR850 that enforces an access control policy between the Internet and the LAN for protection.

Firmware

Code written onto read-only memory (ROM) or programmable read-only memory (PROM). Once firmware has been written onto the ROM or PROM, it is retained even when the device is turned off. Firmware is upgradeable.

FTP

File Transfer Protocol is a standard Internet protocol for exchanging files between computers. FTP is commonly used to download programs and other files to a computer from web pages on Internet servers.

G**Gateway**

A device that enables communication between networks using different protocols. See also *router*.

The WR850 enables up to 253 computers supporting IEEE 802.11b/g or Ethernet to share a single broadband Internet connection.

GUI

Graphical User Interface

H**Hexadecimal**

A base-sixteen numbering system that uses sixteen sequential numbers (0 to 9 and the letters A to F) as base units before adding a new position. On computers, hexadecimal is a convenient way to express binary numbers.

Host

In IP, a host is any computer supporting end-user applications or services with full two-way network access. Each host has a unique host number that combined with the network number forms its IP address.

Host also can mean:

- A computer running a web server that serves pages for one or more web sites belonging to organization(s) or individuals
- A company that provides this service
- In IBM environments, a mainframe computer

I**ICMP**

Internet Control Message Protocol is a protocol used for error, problem, and informational messages sent between IP hosts and gateways. ICMP messages are processed by the IP software and are not usually apparent to the end-user.

IEEE

The Institute of Electrical and Electronics Engineers, Inc. (<http://www.ieee.org>) is an organization that produces standards, technical papers, and symposiums for the electrical and electronic industries and is accredited by ANSI. 802.11b and 802.11g are examples of standards they have produced.

Internet

A worldwide collection of interconnected networks using TCP/IP.

IP

Internet Protocol is a set of standards that enable different types of computers to communicate with one another and exchange data through the Internet. IP provides the appearance of a single, seamless communication system and makes the Internet a virtual network.

IP Address

A unique 32-bit value that identifies each host on a TCP/IP network. TCP/IP networks route messages based on the destination IP address.

For a Class C network, the first 24 bits are the network address and the final 8 bits are the host address; in dotted-decimal format it appears "network.network.network.host."

ISDN

Integrated Services Digital Network

ISP

Internet Service Provider

L**LAN**

Local Area Network. A local area network provides a full-time, high-bandwidth connection over a limited area such as a home, building, or campus. Ethernet is the most widely used LAN standard.

M**MAC Address**

The Media Access Control address is a unique, 48-bit value permanently saved in the ROM at the factory to identify each Ethernet network device. It is expressed as a sequence of 12 hexadecimal digits printed on the unit's label. You need to provide the MAC Address to the cable service provider. Also

called an Ethernet address, physical address, hardware address, or NIC address.

MB

One megabyte; equals 1,024 x 1,024 bytes, 1,024 kilobytes, or about 8 million bits.

Mbps

Million bits per second (megabits per second). A rate of data transfer.

MTU

The Maximum Transmission Unit is the largest amount of data that can be transmitted in one discrete message on a given physical network. The MTU places an upper bound limit on the size of a message that can be transferred by the network in a single frame. Messages exceeding the MTU must be fragmented before transmission, and reassembled at the destination.

Multicast

A data transmission sent from one sender to multiple receivers. See also broadcast and unicast.

N**NAT**

Network Address Translation is an Internet standard for a LAN to use one set of IP addresses for internal traffic and a second set of IP addresses for external traffic.

Network

Two or more computers connected to communicate with each other. Networks have traditionally been connected using some kind of wiring.

NIC

A Network Interface Card converts computer data to serial data in a packet format that it sends over the LAN. A NIC is installed in an expansion slot or can be built-in. Every Ethernet NIC has a MAC address permanently saved in its ROM.

P**Packet**

The unit of data that is routed between the sender and destination on the Internet or other packet-switched network.

PCMCIA

The Personal Computer Memory Card International Association sets international standards for connecting peripherals to portable computers. Laptop computers typically have a PCMCIA slot that can hold one or two PC Cards to provide features such as Ethernet connectivity.

ping

A network function that tests host reachability by sending a small packet to the host and waiting for a reply. If you ping a computer IP address and receive a reply, you know the computer is reachable over the network. It also stands for “Packet InterNet Groper.”

Port Triggering

A mechanism that allows incoming communication with specified applications.

PPP

Point-to-Point Protocol is used to transport other protocols, typically for simple links over serial lines. It is most commonly used to access the Internet with a dial-up modem.

PPPoE

Point-to-Point Protocol over Ethernet. Used by many DSL Internet Service Providers for broadband connection.

PPTP

Point-to-Point Tunneling Protocol encapsulates other protocols. It is a new technology to create VPNs developed jointly by several vendors.

Private IP Address

An IP address assigned to a computer on the WR850 LAN by the DHCP server for a specified lease time. Private IP addresses are invisible to devices on the Internet. See also *Public IP Address*.

Protocol

A formal set of rules and conventions for exchanging data. Different computer types (for example PC, UNIX®, or mainframe) can communicate if they support common protocols.

Public IP Address

The IP address assigned to the WR850 by the service provider. A public IP address is visible to devices on the Internet. See also *Private IP Address*.

R**RJ-11**

The most common type of connector for household or office phones.

RJ-45

An 8-pin modular connector; the most common connector type for 10Base-T or 100Base-T Ethernet networks.

Roaming

The ability to transfer your wireless session from one AP to another AP seamlessly.

ROM

Read-Only Memory.

Router

On IP networks, a device connecting at least two networks, which may or may not be similar. A router is typically located at a gateway between networks. A router operates on OSI network Layer 3. It filters packets based on the IP address, examining the source and destination IP addresses to determine the best route to forward them.

A router is often included as part of a network switch. A router can also be implemented as software on a computer.

Routing Table

A table listing available routes that is used by a router to determine the best route for a packet.

RTS

Request To Send.

S**Server**

In a client/server architecture, a dedicated computer that supplies files or services such as file transfer, remote login, or printing to clients. Also see *client*.

Service Provider

A company providing Internet connection services to subscribers.

SMTP

Simple Mail Transfer Protocol is a standard Internet protocol for transferring e-mail.

Static IP Address

An IP address that is permanently assigned to a host. Normally, a static IP address must be assigned manually. The opposite of *Dynamic IP Address*.

Station

IEEE 802.11b term for wireless client.

Subscriber

A user who accesses television, data, or other services from a service provider.

Subnet Mask

A methodology that determines what the router will examine for in determining the destination of an IP address. A router delivers packets using the network address.

Switch

On an Ethernet network, a switch filters frames based on the MAC address, in a manner similar to a bridge. A switch is more advanced because it can connect more than two segments.

T**TCP**

Transmission Control Protocol on OSI Transport Layer 4 provides reliable transport over the network for data transmitted using IP (network layer three). It is an end-to-end protocol defining rules and procedures for data exchange between hosts on top of connectionless IP. TCP uses a timer to track outstanding packets, checks error in incoming packets, and retransmits packets if requested.

TCP/IP

The Transmission Control Protocol/Internet Protocol suite provides standards and rules for data communication between networks on the Internet. It is the worldwide Internetworking standard and the basic communications protocol of the Internet.

Tunnel

To place packets inside other packets to send over a network. The protocol of the enclosing packet is understood by each endpoint, or tunnel interface, where the packet enters and exits the network. VPNs rely on tunneling to create a secure network.

Tunneling requires the following protocol types:

- A carrier protocol, such as TCP, used by the network that the data travels over
- An encapsulating protocol, such as IPSec, L2TP, or PPTP, that is wrapped around the original data
- A passenger protocol, such as IP, for the original data

U**UDP**

User Datagram Protocol. A method used along with the IP to send data in the form of message units (datagram) between network devices over a LAN or WAN.

Unicast

A point-to-point data transmission sent from one sender to one receiver. This is the normal way you access websites. See also *multicast*.

UPnP

Universal Plug and Play

USB

Universal Serial Bus is a computer interface for add-on devices such as printers, scanners, mice, modems, or keyboards. USB supports data transfer rates of 12 Mbps and plug-and-play installation. You can connect up to 127 devices to a single USB port.

V**VoIP**

Voice over Internet Protocol is a method to exchange voice, fax, and other information over the Internet. Voice and fax have traditionally been carried over traditional telephone lines of the PSTN (Public Switched Telephone Network) using a dedicated circuit for each line. VoIP enables calls to travel as discrete data packets on shared lines. VoIP is an important part of the convergence of computers, telephones, and television into a single integrated information network.

VPN

A virtual private network is a private network that uses “virtual” connections (tunnels) routed over a public network (usually the Internet) to provide a secure and fast connection; usually to users working remotely at home or in small branch offices. A VPN connection provides security and performance similar to a dedicated link (for example, a leased line), but at much lower cost.

W**WAN**

A wide-area network provides a connection over a large geographic area, such as a country or the whole world. The bandwidth depends on need and cost, but is usually much lower than for a LAN.

WAP

Wireless Access Point or Wireless Access Protocol. See also *Access Point*.

WEP

Wired Equivalent Privacy encryption protects the privacy of data transmitted over a wireless LAN. WEP uses keys to encrypt and decrypt transmitted data. The access point must authenticate a client before it can transfer data to another client. WEP is part of IEEE 802.11b.

Wi-Fi

Wireless fidelity (pronounced why'-fy) brand name applied to products supporting IEEE 802.11b/g.

WLAN

Wireless LAN.

WME

Wireless Media Extensions (WME) is another acronym commonly used for WMM features.

WMM

Wi-Fi Multimedia, which optimizes the multimedia (e.g., voice, video) sharing over the network.

WPA

Wi-Fi Protected Access. A security regimen developed by IEEE for protection of data on a WLAN.

WWW

World Wide Web. An interface to the Internet that you use to navigate and hyperlink to information.

Visit our website at:
www.motorola.com/broadband



520075-001
08/05

MGBI